

# NWA3550

*IEEE 802.11a/b/g Outdoor WLAN Access Point*

## ***User's Guide***

Version 3.60

4/2008

Edition 1

### **DEFAULT LOGIN**

|                   |                           |
|-------------------|---------------------------|
| <b>IP Address</b> | <b>http://192.168.1.2</b> |
| <b>Password</b>   | <b>1234</b>               |

---

**ZyXEL**  
[www.zyxel.com](http://www.zyxel.com)



# About This User's Guide

## Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

## Related Documentation

- Quick Start Guide  
The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Supporting Disk  
Refer to the included CD for support documents.
- ZyXEL Web Site  
Please refer to [www.zyxel.com](http://www.zyxel.com) for additional support documentation and product certifications.

## User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,  
ZyXEL Communications Corp.,  
6 Innovation Road II,  
Science-Based Industrial Park,  
Hsinchu, 300, Taiwan.  
E-mail: [techwriters@zyxel.com.tw](mailto:techwriters@zyxel.com.tw)

# Document Conventions

## Warnings and Notes

These are how warnings and notes are shown in this User's Guide.



---

Warnings tell you about things that could harm you or your device.

---



---

Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.






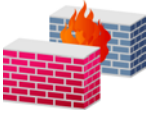



---

## Syntax Conventions

- The NWA3550 may be referred to as the “ZyXEL Device”, the “device” or the “system” in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the “enter” or “return” key on your keyboard.
- “Enter” means for you to type one or more characters and then press the [ENTER] key. “Select” or “choose” means for you to use one of the predefined choices.
- A right angle bracket ( > ) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the “metric” value or the “scientific” value. For example, “k” for kilo may denote “1000” or “1024”, “M” for mega may denote “1000000” or “1048576” and so on.
- “e.g.” is a shorthand for “for instance”, and “i.e.” means “that is” or “in other words”.

## Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyXEL Device icon is not an exact representation of your device.

|   |   |  |
|---|---|--|
| ZyXEL Device<br> | Computer<br> | Notebook computer<br> |
| Server<br>       | DSLAM<br>    | Firewall<br>          |
| Telephone<br>    | Switch<br>   | Router<br>            |

# Safety Warnings



---

For your safety, be sure to read and follow all warning notices and instructions.

---

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- ONLY qualified service personnel should service or disassemble this device.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- The PoE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.
- Please select an antenna that conforms with your local radio regulations. ZyXEL bears no responsibility whatsoever for cases of illegal installation.

This product is recyclable. Dispose of it properly.





# Contents Overview

|  |            |
|--|------------|
| <b>Introduction .....</b>                            | <b>31</b>  |
| Introducing the ZyXEL Device .....                   | 33         |
| Introducing the Web Configurator .....               | 41         |
| Status Screens .....                                 | 45         |
| Tutorial .....                                       | 49         |
| <b>The Web Configurator .....</b>                    | <b>77</b>  |
| System Screens .....                                 | 79         |
| Wireless Configuration .....                         | 85         |
| Wireless Security Configuration .....                | 101        |
| MBSSID and SSID .....                                | 113        |
| Other Wireless Configuration .....                   | 121        |
| IP Screen .....                                      | 133        |
| Rogue AP .....                                       | 137        |
| Remote Management Screens .....                      | 143        |
| Internal RADIUS Server .....                         | 161        |
| Certificates .....                                   | 169        |
| Log Screens .....                                    | 187        |
| VLAN .....   | 195        |
| Maintenance .....                                    | 213        |
| <b>SMT, Troubleshooting and Specifications .....</b> | <b>223</b> |
| Introducing the SMT .....                            | 225        |
| General Setup .....                                  | 231        |
| LAN Setup .....                                      | 233        |
| System Password .....                                | 235        |
| System Information and Diagnosis .....               | 237        |
| Firmware and Configuration File Maintenance .....    | 243        |
| System Maintenance and Information .....             | 249        |
| Troubleshooting .....                                | 257        |
| Product Specifications .....                         | 261        |
| <b>Appendices and Index .....</b>                    | <b>267</b> |



# Table of Contents

|                                      |           |
|--------------------------------------|-----------|
| <b>About This User's Guide .....</b> | <b>3</b>  |
| <b>Document Conventions.....</b>     | <b>4</b>  |
| <b>Safety Warnings.....</b>          | <b>6</b>  |
| <b>Contents Overview .....</b>       | <b>9</b>  |
| <b>Table of Contents.....</b>        | <b>11</b> |
| <b>List of Figures .....</b>         | <b>21</b> |
| <b>List of Tables.....</b>           | <b>27</b> |

## **Part I: Introduction..... 31**

### **Chapter 1** **Introducing the ZyXEL Device ..... 33**

|   |    |
|---|----|
| 1.1 Introducing the ZyXEL Device .....                      | 33 |
| 1.2 Applications for the ZyXEL Device .....                 | 33 |
| 1.2.1 Access Point .....                                    | 34 |
| 1.2.2 Bridge / Repeater .....                               | 34 |
| 1.2.3 AP + Bridge .....                                     | 35 |
| 1.2.4 MBSSID .....  | 36 |
| 1.2.5 Pre-Configured SSID Profiles .....                    | 37 |
| 1.2.6 Configuring Dual WLAN Adaptors .....                  | 37 |
| 1.3 Ways to Manage the ZyXEL Device .....                   | 38 |
| 1.4 Configuring Your ZyXEL Device's Security Features ..... | 38 |
| 1.4.1 Control Access to Your Device .....                   | 38 |
| 1.4.2 Wireless Security .....                               | 39 |
| 1.5 Maintaining Your ZyXEL Device .....                     | 39 |
| 1.6 Hardware Connections .....                              | 40 |

### **Chapter 2** **Introducing the Web Configurator ..... 41**

|   |    |
|---|----|
| 2.1 Accessing the Web Configurator .....          | 41 |
| 2.2 Resetting the ZyXEL Device .....              | 42 |
| 2.2.1 Methods of Restoring Factory-Defaults ..... | 43 |
| 2.3 Navigating the Web Configurator .....         | 43 |

|  |           |
|--|-----------|
| <b>Chapter 3</b>   |           |
| <b>Status Screens .....</b>                                      | <b>45</b> |
| 3.1 The Status Screen .....                                      | 45        |
| <b>Chapter 4</b>   |           |
| <b>Tutorial .....</b>  | <b>49</b> |
| 4.1 How to Configure the Wireless LAN .....                      | 49        |
| 4.1.1 Choosing the Wireless Mode .....                           | 49        |
| 4.1.1.1 Configuring Dual WLAN Adaptors .....                     | 49        |
| 4.1.2 Wireless LAN Configuration Overview .....                  | 50        |
| 4.1.3 Further Reading .....                                      | 52        |
| 4.2 How to Configure Multiple Wireless Networks .....            | 52        |
| 4.2.1 Change the Operating Mode .....                            | 53        |
| 4.2.2 Configure the VoIP Network .....                           | 55        |
| 4.2.2.1 Set Up Security for the VoIP Profile .....               | 56        |
| 4.2.2.2 Activate the VoIP Profile .....                          | 58        |
| 4.2.3 Configure the Guest Network .....                          | 58        |
| 4.2.3.1 Set Up Security for the Guest Profile .....              | 59        |
| 4.2.3.2 Set up Layer 2 Isolation .....                           | 60        |
| 4.2.3.3 Activate the Guest Profile .....                         | 61        |
| 4.2.4 Testing the Wireless Networks .....                        | 62        |
| 4.3 How to Set Up and Use Rogue AP Detection .....               | 62        |
| 4.3.1 Set Up and Save a Friendly AP list .....                   | 64        |
| 4.3.2 Activate Periodic Rogue AP Detection .....                 | 67        |
| 4.3.3 Set Up E-mail Logs .....                                   | 67        |
| 4.3.4 Configure Your Other Access Points .....                   | 68        |
| 4.3.5 Test the Setup .....                                       | 69        |
| 4.4 Using Multiple MAC Filters and L-2 Isolation Profiles .....  | 69        |
| 4.4.1 Scenario .....   | 70        |
| 4.4.2 Your Requirements .....                                    | 70        |
| 4.4.3 Setup .....  | 70        |
| 4.4.4 Configure the SERVER_1 Network .....                       | 71        |
| 4.4.5 Configure the SERVER_2 Network .....                       | 73        |
| 4.4.6 Checking your Settings and Testing the Configuration ..... | 74        |
| 4.4.6.1 Checking Settings .....                                  | 74        |
| 4.4.6.2 Testing the Configuration .....                          | 75        |
| <b>Part II: The Web Configurator .....</b>                       | <b>77</b> |
| <b>Chapter 5</b>   |           |
| <b>System Screens .....</b>                                      | <b>79</b> |

|  |            |
|--|------------|
| 5.1 System Overview .....                        | 79         |
| 5.2 Configuring General Setup .....              | 79         |
| 5.3 Administrator Authentication on RADIUS ..... | 80         |
| 5.3.1 Configuring the Password .....             | 80         |
| 5.4 Configuring Time Setting .....               | 82         |
| 5.5 Pre-defined NTP Time Servers List .....      | 84         |
| <b>Chapter 6</b>                                 |            |
| <b>Wireless Configuration.....</b>               | <b>85</b>  |
| 6.1 Wireless Network Overview .....              | 85         |
| 6.2 Wireless LAN Basics .....                    | 86         |
| 6.3 Quality of Service .....                     | 86         |
| 6.3.1 WMM QoS .....                              | 86         |
| 6.3.1.1 WMM QoS Priorities .....                 | 87         |
| 6.3.2 ATC .....                                  | 87         |
| 6.3.3 ATC+WMM .....                              | 88         |
| 6.3.3.1 ATC+WMM from LAN to WLAN .....           | 88         |
| 6.3.3.2 ATC+WMM from WLAN to LAN .....           | 88         |
| 6.3.4 Type Of Service (ToS) .....                | 89         |
| 6.3.4.1 DiffServ .....                           | 89         |
| 6.3.4.2 DSCP and Per-Hop Behavior .....          | 89         |
| 6.3.5 ToS (Type of Service) and WMM QoS .....    | 89         |
| 6.4 Spanning Tree Protocol (STP) .....           | 90         |
| 6.4.1 Rapid STP .....                            | 90         |
| 6.4.2 STP Terminology .....                      | 90         |
| 6.4.3 How STP Works .....                        | 91         |
| 6.4.4 STP Port States .....                      | 91         |
| 6.5 DFS .....                                    | 91         |
| 6.6 Wireless Screen Overview .....               | 92         |
| 6.7 Configuring Wireless Settings .....          | 92         |
| 6.7.1 Access Point Mode .....                    | 92         |
| 6.7.2 Bridge/Repeater Mode .....                 | 94         |
| 6.7.3 AP+Bridge Mode .....                       | 98         |
| 6.7.4 MBSSID Mode .....                          | 99         |
| <b>Chapter 7</b>                                 |            |
| <b>Wireless Security Configuration .....</b>     | <b>101</b> |
| 7.1 Wireless Security Overview .....             | 101        |
| 7.1.1 SSID .....                                 | 101        |
| 7.1.2 MAC Address Filter .....                   | 101        |
| 7.1.3 User Authentication .....                  | 102        |
| 7.1.4 Encryption .....                           | 102        |
| 7.2 Security Modes .....                         | 103        |

|   |            |
|---|------------|
| 7.3 Configuring Security .....                                    | 103        |
| 7.3.1 Security: WEP .....   | 104        |
| 7.3.2 Security: 802.1x Only .....                                 | 105        |
| 7.3.3 Security: 802.1x Static 64-bit, 802.1x Static 128-bit ..... | 106        |
| 7.3.4 Security: WPA .....   | 108        |
| 7.3.5 Security: WPA2 or WPA2-MIX .....                            | 108        |
| 7.3.6 Security: WPA-PSK, WPA2-PSK, WPA2-PSK-MIX .....             | 110        |
| 7.4 Introduction to RADIUS .....                                  | 111        |
| 7.5 Configuring RADIUS .....                                      | 111        |
| <br><b>Chapter 8</b>  |            |
| <b>MBSSID and SSID .....</b>                                      | <b>113</b> |
| 8.1 Wireless LAN Infrastructures .....                            | 113        |
| 8.1.1 MBSSID .....  | 113        |
| 8.1.2 Notes on Multiple BSS .....                                 | 113        |
| 8.1.3 Multiple BSS Example .....                                  | 113        |
| 8.1.4 Multiple BSS with VLAN Example .....                        | 113        |
| 8.1.5 Configuring Multiple BSSs .....                             | 114        |
| 8.2 SSID .....  | 117        |
| 8.2.1 The SSID Screen .....                                       | 117        |
| 8.2.2 Configuring SSID .....                                      | 118        |
| <br><b>Chapter 9</b>  |            |
| <b>Other Wireless Configuration .....</b>                         | <b>121</b> |
| 9.1 Layer-2 Isolation Introduction .....                          | 121        |
| 9.2 The Layer-2 Isolation Screen .....                            | 122        |
| 9.3 Configuring Layer-2 Isolation .....                           | 123        |
| 9.3.1 Layer-2 Isolation Examples .....                            | 125        |
| 9.3.1.1 Layer-2 Isolation Example 1 .....                         | 125        |
| 9.3.1.2 Layer-2 Isolation Example 2 .....                         | 126        |
| 9.4 The MAC Filter Screen .....                                   | 126        |
| 9.4.1 Configuring MAC Filtering .....                             | 127        |
| 9.5 Configuring Roaming .....                                     | 129        |
| 9.5.1 Requirements for Roaming .....                              | 130        |
| <br><b>Chapter 10</b>   |            |
| <b>IP Screen.....</b>   | <b>133</b> |
| 10.1 Factory Ethernet Defaults .....                              | 133        |
| 10.2 TCP/IP Parameters .....                                      | 133        |
| 10.2.1 WAN IP Address Assignment .....                            | 133        |
| 10.3 Configuring IP Settings .....                                | 134        |
| <br><b>Chapter 11</b>   |            |
| <b>Rogue AP.....</b>  | <b>137</b> |

|  |            |
|--|------------|
| 11.1 Rogue AP Introduction .....                   | 137        |
| 11.2 Rogue AP Examples .....                       | 137        |
| 11.2.1 "Honeypot" Attack .....                     | 138        |
| 11.3 Configuring Rogue AP Detection .....          | 139        |
| 11.3.1 Rogue AP: Configuration .....               | 139        |
| 11.3.2 Rogue AP: Friendly AP .....                 | 140        |
| 11.3.3 Rogue AP List .....                         | 141        |
| <b>Chapter 12</b>                                  |            |
| <b>Remote Management Screens .....</b>             | <b>143</b> |
| 12.1 Remote Management Overview .....              | 143        |
| 12.1.1 Remote Management Limitations .....         | 143        |
| 12.1.2 System Timeout .....                        | 144        |
| 12.2 SSH .....                                     | 144        |
| 12.3 How SSH Works .....                           | 144        |
| 12.4 SSH Implementation on the ZyXEL Device .....  | 145        |
| 12.4.1 Requirements for Using SSH .....            | 145        |
| 12.5 Configuring Telnet .....                      | 145        |
| 12.6 Configuring FTP .....                         | 147        |
| 12.7 WWW (HTTP and HTTPS) .....                    | 148        |
| 12.8 Configuring WWW .....                         | 149        |
| 12.9 HTTPS Example .....                           | 150        |
| 12.9.1 Internet Explorer Warning Messages .....    | 150        |
| 12.9.2 Netscape Navigator Warning Messages .....   | 151        |
| 12.9.3 Avoiding the Browser Warning Messages ..... | 151        |
| 12.9.4 Login Screen .....                          | 152        |
| 12.10 SNMP .....                                   | 154        |
| 12.10.1 Supported MIBs .....                       | 156        |
| 12.10.2 SNMP Traps .....                           | 156        |
| 12.11 SNMP Trap Interface Index .....              | 157        |
| 12.11.1 SNMP v3 and Security .....                 | 157        |
| 12.11.2 Configuring SNMP .....                     | 157        |
| 12.11.2.1 The SNMPv3 User Profile Screen .....     | 159        |
| <b>Chapter 13</b>                                  |            |
| <b>Internal RADIUS Server .....</b>                | <b>161</b> |
| 13.1 Internal RADIUS Overview .....                | 161        |
| 13.2 Internal RADIUS Server Setting .....          | 161        |
| 13.3 Trusted AP Overview .....                     | 163        |
| 13.4 Configuring Trusted AP .....                  | 164        |
| 13.5 Configuring Trusted Users .....               | 166        |
| <b>Chapter 14</b>                                  |            |
| <b>Certificates .....</b>                          | <b>169</b> |

|   |            |
|---|------------|
| 14.1 Certificates Overview .....  | 169        |
| 14.1.1 Advantages of Certificates .....                                 | 170        |
| 14.2 Self-signed Certificates .....                                     | 170        |
| 14.3 Verifying a Certificate .....                                      | 170        |
| 14.3.1 Checking the Fingerprint of a Certificate on Your Computer ..... | 170        |
| 14.4 Configuration Summary .....  | 171        |
| 14.5 My Certificates .....  | 171        |
| 14.6 Certificate File Formats .....                                     | 173        |
| 14.7 Importing a Certificate .....                                      | 174        |
| 14.8 Creating a Certificate .....                                       | 175        |
| 14.9 My Certificate Details .....                                       | 177        |
| 14.10 Trusted CAs .....   | 180        |
| 14.11 Importing a Trusted CA's Certificate .....                        | 181        |
| 14.12 Trusted CA Certificate Details .....                              | 182        |
| <br><b>Chapter 15</b>   |            |
| <b>Log Screens .....</b>  | <b>187</b> |
| 15.1 Configuring View Log .....   | 187        |
| 15.2 Configuring Log Settings .....                                     | 188        |
| 15.3 Example Log Messages .....   | 190        |
| 15.4 Log Commands .....   | 192        |
| 15.4.1 Configuring What You Want the ZyXEL Device to Log .....          | 192        |
| 15.4.2 Displaying Logs .....  | 192        |
| 15.5 Log Command Example .....  | 193        |
| <br><b>Chapter 16</b>   |            |
| <b>VLAN .....</b>   | <b>195</b> |
| 16.1 VLAN .....   | 195        |
| 16.1.1 Management VLAN ID .....   | 195        |
| 16.1.2 VLAN Tagging .....   | 195        |
| 16.2 Configuring VLAN .....   | 196        |
| 16.2.1 Wireless VLAN .....  | 196        |
| 16.2.2 RADIUS VLAN .....  | 198        |
| 16.2.3 Configuring Management VLAN Example .....                        | 199        |
| 16.2.4 Configuring Microsoft's IAS Server Example .....                 | 202        |
| 16.2.4.1 Configuring VLAN Groups .....                                  | 202        |
| 16.2.4.2 Configuring Remote Access Policies .....                       | 203        |
| 16.2.5 Second Rx VLAN ID Example .....                                  | 210        |
| 16.2.5.1 Second Rx VLAN Setup Example .....                             | 210        |
| <br><b>Chapter 17</b>   |            |
| <b>Maintenance .....</b>  | <b>213</b> |
| 17.1 Maintenance Overview .....   | 213        |

|   |            |
|---|------------|
| 17.2 System Status Screen .....                                   | 213        |
| 17.2.1 System Statistics .....                                    | 214        |
| 17.3 Association List .....                                       | 215        |
| 17.4 Channel Usage .....  | 216        |
| 17.5 F/W Upload Screen .....                                      | 217        |
| 17.6 Configuration Screen .....                                   | 219        |
| 17.6.1 Backup Configuration .....                                 | 220        |
| 17.6.2 Restore Configuration .....                                | 220        |
| 17.6.3 Back to Factory Defaults .....                             | 222        |
| 17.7 Restart Screen .....   | 222        |
| <br><b>Part III: SMT, Troubleshooting and Specifications.....</b> | <b>223</b> |
| <br><b>Chapter 18</b>   |            |
| <b>Introducing the SMT .....</b>                                  | <b>225</b> |
| 18.1 Introduction to the SMT .....                                | 225        |
| 18.2 Accessing the SMT via the Console Port .....                 | 225        |
| 18.2.1 Initial Screen .....                                       | 225        |
| 18.2.2 Entering the Password .....                                | 226        |
| 18.3 Connect to your ZyXEL Device Using Telnet .....              | 227        |
| 18.4 Changing the System Password .....                           | 227        |
| 18.5 SMT Menu Overview Example .....                              | 228        |
| 18.6 Navigating the SMT Interface .....                           | 228        |
| 18.6.1 System Management Terminal Interface Summary .....         | 230        |
| <br><b>Chapter 19</b>   |            |
| <b>General Setup.....</b>   | <b>231</b> |
| 19.1 General Setup .....  | 231        |
| 19.1.1 Procedure To Configure Menu 1 .....                        | 231        |
| <br><b>Chapter 20</b>   |            |
| <b>LAN Setup.....</b>   | <b>233</b> |
| 20.1 LAN Setup .....  | 233        |
| 20.2 TCP/IP Ethernet Setup .....                                  | 233        |
| <br><b>Chapter 21</b>   |            |
| <b>System Password .....</b>                                      | <b>235</b> |
| 21.1 System Password .....  | 235        |
| <br><b>Chapter 22</b>   |            |
| <b>System Information and Diagnosis.....</b>                      | <b>237</b> |

|  |            |
|--|------------|
| 22.1 System Status .....   | 237        |
| 22.2 System Information .....  | 238        |
| 22.2.1 System Information .....  | 239        |
| 22.2.2 Console Port Speed .....  | 240        |
| 22.3 Log and Trace .....   | 240        |
| 22.3.1 Viewing Error Log .....   | 240        |
| 22.4 Diagnostic .....  | 241        |
| <br><b>Chapter 23</b>  |            |
| <b>Firmware and Configuration File Maintenance .....</b>                   | <b>243</b> |
| 23.1 Filename Conventions .....  | 243        |
| 23.2 Backup Configuration .....  | 244        |
| 23.2.1 Using the FTP command from the DOS Prompt .....                     | 244        |
| 23.2.2 Backup Configuration Using TFTP .....                               | 245        |
| 23.2.3 Example: TFTP Command .....   | 246        |
| 23.3 Restore Configuration .....   | 246        |
| 23.3.1 Using the FTP command from the DOS Prompt Example .....             | 246        |
| 23.3.2 TFTP File Upload .....  | 247        |
| 23.3.3 Example: TFTP Command .....   | 248        |
| <br><b>Chapter 24</b>  |            |
| <b>System Maintenance and Information .....</b>                            | <b>249</b> |
| 24.1 Command Interpreter Mode .....  | 249        |
| 24.1.1 Command Syntax .....  | 250        |
| 24.1.2 Command Usage .....   | 250        |
| 24.1.3 Brute-Force Password Guessing Protection .....                      | 250        |
| 24.1.3.1 Configuring Brute-Force Password Guessing Protection: Example 250 |            |
| 24.2 Time and Date Setting .....   | 251        |
| 24.2.1 Resetting the Time .....  | 252        |
| 24.3 Remote Management Setup .....   | 252        |
| 24.3.1 Telnet .....  | 252        |
| 24.3.2 FTP .....   | 253        |
| 24.3.3 Web .....   | 253        |
| 24.3.4 Remote Management Setup .....                                       | 253        |
| 24.3.5 Remote Management Limitations .....                                 | 254        |
| 24.4 System Timeout .....  | 255        |
| <br><b>Chapter 25</b>  |            |
| <b>Troubleshooting .....</b>   | <b>257</b> |
| 25.1 Power and Hardware Connections .....                                  | 257        |
| 25.2 ZyXEL Device Access and Login .....                                   | 257        |
| 25.3 Internet Access .....   | 259        |
| 25.4 Wireless Router/AP Troubleshooting .....                              | 260        |

|   |            |
|---|------------|
| <b>Chapter 26</b>   |            |
| <b>Product Specifications .....</b>                               | <b>261</b> |
| <br>  |            |
| <b>Part IV: Appendices and Index .....</b>                        | <b>267</b> |
| <br>  |            |
| Appendix A Setting up Your Computer's IP Address.....             | 269        |
| Appendix B Wireless LANs .....                                    | 281        |
| Appendix C Pop-up Windows, JavaScripts and Java Permissions ..... | 295        |
| Appendix D IP Addresses and Subnetting .....                      | 301        |
| Appendix E Text File Based Auto Configuration.....                | 309        |
| Appendix F Legal Information .....                                | 317        |
| Appendix G Customer Support .....                                 | 321        |
| <b>Index.....</b>   | <b>327</b> |



# List of Figures

|   |    |
|---|----|
| Figure 1 Access Point Application .....                   | 34 |
| Figure 2 Bridge Application .....                         | 35 |
| Figure 3 Repeater Application .....                       | 35 |
| Figure 4 AP+Bridge Application .....                      | 36 |
| Figure 5 Multiple BSSs .....                              | 37 |
| Figure 6 Dual WLAN Adaptors Example .....                 | 38 |
| Figure 7 Change Password Screen .....                     | 42 |
| Figure 8 Replace Certificate Screen .....                 | 42 |
| Figure 9 The Status Screen of the Web Configurator .....  | 43 |
| Figure 10 The Status Screen .....                         | 45 |
| Figure 11 Configuring Wireless LAN .....                  | 51 |
| Figure 12 Tutorial: Example MBSSID Setup .....            | 53 |
| Figure 13 Tutorial: Wireless LAN: Before .....            | 54 |
| Figure 14 Tutorial: Wireless LAN: Change Mode .....       | 54 |
| Figure 15 Tutorial: WIRELESS > SSID .....                 | 55 |
| Figure 16 Tutorial: VoIP SSID Profile Edit .....          | 56 |
| Figure 17 Tutorial: VoIP Security .....                   | 57 |
| Figure 18 Tutorial: VoIP Security Profile Edit .....      | 57 |
| Figure 19 Tutorial: VoIP Security: Updated .....          | 58 |
| Figure 20 Tutorial: Activate VoIP Profile .....           | 58 |
| Figure 21 Tutorial: Guest Edit .....                      | 59 |
| Figure 22 Tutorial: Guest Security Profile Edit .....     | 59 |
| Figure 23 Tutorial: Guest Security: Updated .....         | 60 |
| Figure 24 Tutorial: Layer 2 Isolation .....               | 60 |
| Figure 25 Tutorial: Layer 2 Isolation Profile .....       | 61 |
| Figure 26 Tutorial: Activate Guest Profile .....          | 62 |
| Figure 27 Tutorial: Wireless Network Example .....        | 63 |
| Figure 28 Tutorial: Friendly AP (Before Data Entry) ..... | 64 |
| Figure 29 Tutorial: Friendly AP (After Data Entry) .....  | 65 |
| Figure 30 Tutorial: Configuration .....                   | 66 |
| Figure 31 Tutorial: Warning .....                         | 66 |
| Figure 32 Tutorial: Save Friendly AP list .....           | 66 |
| Figure 33 Tutorial: Periodic Rogue AP Detection .....     | 67 |
| Figure 34 Tutorial: Log Settings .....                    | 68 |
| Figure 35 Tutorial: Example Network .....                 | 70 |
| Figure 36 Tutorial: SSID Profile .....                    | 72 |
| Figure 37 Tutorial: SSID Edit .....                       | 72 |
| Figure 38 Tutorial: Layer-2 Isolation Edit .....          | 73 |

|   |     |
|---|-----|
| Figure 39 Tutorial: MAC Filter Edit (SERVER_1) .....                  | 73  |
| Figure 40 Tutorial: SSID Profiles Activated .....                     | 75  |
| Figure 41 Tutorial: SSID Tab Correct Settings .....                   | 75  |
| Figure 42 System > General .....                                      | 79  |
| Figure 43 SYSTEM > Password. ....                                     | 81  |
| Figure 44 SYSTEM > Time Setting .....                                 | 82  |
| Figure 45 Example of a Wireless Network .....                         | 85  |
| Figure 46 DiffServ: Differentiated Service Field .....                | 89  |
| Figure 47 Wireless: Access Point .....                                | 92  |
| Figure 48 Bridging Example .....                                      | 94  |
| Figure 49 Bridge Loop: Two Bridges Connected to Hub .....             | 95  |
| Figure 50 Bridge Loop: Bridge Connected to Wired LAN .....            | 95  |
| Figure 51 Wireless: Bridge/Repeater .....                             | 96  |
| Figure 52 Wireless: AP+Bridge .....                                   | 98  |
| Figure 53 Wireless > Security .....                                   | 104 |
| Figure 54 WIRELESS > Security: WEP .....                              | 105 |
| Figure 55 Security: 802.1x Only .....                                 | 106 |
| Figure 56 Security: 802.1x Static 64-bit, 802.1x Static 128-bit ..... | 107 |
| Figure 57 Security: WPA .....   | 108 |
| Figure 58 Security:WPA2 or WPA2-MIX .....                             | 109 |
| Figure 59 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX .....           | 110 |
| Figure 60 RADIUS .....  | 111 |
| Figure 61 Multiple BSS with VLAN Example .....                        | 114 |
| Figure 62 Wireless: Multiple BSS .....                                | 115 |
| Figure 63 SSID .....  | 117 |
| Figure 64 Configuring SSID .....                                      | 119 |
| Figure 65 Layer-2 Isolation Application .....                         | 122 |
| Figure 66 WIRELESS > Layer 2 Isolation .....                          | 123 |
| Figure 67 WIRELESS > Layer-2 Isolation Configuration Screen .....     | 124 |
| Figure 68 Layer-2 Isolation Example Configuration .....               | 125 |
| Figure 69 Layer-2 Isolation Example 1 .....                           | 125 |
| Figure 70 Layer-2 Isolation Example 2 .....                           | 126 |
| Figure 71 WIRELESS > MAC Filter .....                                 | 127 |
| Figure 72 MAC Address Filter .....                                    | 128 |
| Figure 73 Roaming Example .....                                       | 130 |
| Figure 74 Roaming .....   | 131 |
| Figure 75 IP Setup .....  | 134 |
| Figure 76 Rogue AP: Example .....                                     | 138 |
| Figure 77 "Honeypot" Attack .....                                     | 139 |
| Figure 78 ROGUE AP > Configuration .....                              | 140 |
| Figure 79 ROGUE AP > Friendly AP .....                                | 141 |
| Figure 80 ROGUE AP > Rogue AP .....                                   | 142 |
| Figure 81 How SSH Works .....   | 144 |

|  |     |
|--|-----|
| Figure 82 Remote Management: Telnet .....                      | 146 |
| Figure 83 Remote Management: FTP .....                         | 147 |
| Figure 84 HTTPS Implementation .....                           | 148 |
| Figure 85 Remote Management: WWW .....                         | 149 |
| Figure 86 Security Alert Dialog Box (Internet Explorer) .....  | 150 |
| Figure 87 Security Certificate 1 (Netscape) .....              | 151 |
| Figure 88 Security Certificate 2 (Netscape) .....              | 151 |
| Figure 89 Example: Lock Denoting a Secure Connection .....     | 153 |
| Figure 90 Replace Certificate .....                            | 153 |
| Figure 91 Device-specific Certificate .....                    | 154 |
| Figure 92 Common ZyXEL Device Certificate .....                | 154 |
| Figure 93 SNMP Management Model .....                          | 155 |
| Figure 94 Remote Management: SNMP .....                        | 158 |
| Figure 95 Remote Management: SNMPv3 User Profile .....         | 159 |
| Figure 96 Internal RADIUS Server Setting Screen .....          | 162 |
| Figure 97 Trusted AP Overview .....                            | 164 |
| Figure 98 Trusted AP Screen .....                              | 165 |
| Figure 99 Trusted Users Screen .....                           | 166 |
| Figure 100 Certificates on Your Computer .....                 | 170 |
| Figure 101 Certificate Details .....                           | 171 |
| Figure 102 My Certificates .....                               | 172 |
| Figure 103 My Certificate Import .....                         | 174 |
| Figure 104 My Certificate Create .....                         | 175 |
| Figure 105 My Certificate Details .....                        | 178 |
| Figure 106 Trusted CAs .....                                   | 180 |
| Figure 107 Trusted CA Import .....                             | 182 |
| Figure 108 Trusted CA Details .....                            | 183 |
| Figure 109 View Log .....                                      | 187 |
| Figure 110 Log Settings .....                                  | 189 |
| Figure 111 Wireless VLAN .....                                 | 197 |
| Figure 112 RADIUS VLAN .....                                   | 198 |
| Figure 113 Management VLAN Configuration Example .....         | 200 |
| Figure 114 VLAN-Aware Switch - Static VLAN .....               | 200 |
| Figure 115 VLAN-Aware Switch .....                             | 200 |
| Figure 116 VLAN-Aware Switch - VLAN Status .....               | 201 |
| Figure 117 VLAN Setup .....                                    | 201 |
| Figure 118 New Global Security Group .....                     | 203 |
| Figure 119 Add Group Members .....                             | 203 |
| Figure 120 New Remote Access Policy for VLAN Group .....       | 204 |
| Figure 121 Specifying Windows-Group Condition .....            | 204 |
| Figure 122 Adding VLAN Group .....                             | 205 |
| Figure 123 Granting Permissions and User Profile Screens ..... | 205 |
| Figure 124 Authentication Tab Settings .....                   | 206 |

|  |     |
|--|-----|
| Figure 125 Encryption Tab Settings .....                                   | 206 |
| Figure 126 Connection Attributes Screen .....                              | 207 |
| Figure 127 RADIUS Attribute Screen .....                                   | 207 |
| Figure 128 802 Attribute Setting for Tunnel-Medium-Type .....              | 208 |
| Figure 129 VLAN ID Attribute Setting for Tunnel-Pvt-Group-ID .....         | 208 |
| Figure 130 VLAN Attribute Setting for Tunnel-Type .....                    | 209 |
| Figure 131 Completed Advanced Tab .....                                    | 209 |
| Figure 132 Second Rx VLAN ID Example .....                                 | 210 |
| Figure 133 Configuring SSID: Second Rx VLAN ID Example .....               | 211 |
| Figure 134 System Status .....   | 213 |
| Figure 135 System Status: Show Statistics .....                            | 214 |
| Figure 136 Association List .....  | 216 |
| Figure 137 Channel Usage .....   | 217 |
| Figure 138 Firmware Upload .....   | 218 |
| Figure 139 Firmware Upload In Process .....                                | 218 |
| Figure 140 Network Temporarily Disconnected .....                          | 219 |
| Figure 141 Firmware Upload Error .....                                     | 219 |
| Figure 142 Configuration .....   | 220 |
| Figure 143 Configuration Upload Successful .....                           | 221 |
| Figure 144 Network Temporarily Disconnected .....                          | 221 |
| Figure 145 Configuration Upload Error .....                                | 221 |
| Figure 146 Reset Warning Message .....                                     | 222 |
| Figure 147 Restart Screen .....  | 222 |
| Figure 148 Initial Screen .....  | 226 |
| Figure 149 Password Screen .....   | 227 |
| Figure 150 Login Screen .....  | 227 |
| Figure 151 Menu 23 System Password .....                                   | 228 |
| Figure 152 SMT Main Menu .....   | 229 |
| Figure 153 Menu 1 General Setup .....                                      | 231 |
| Figure 154 Menu 3 LAN Setup .....  | 233 |
| Figure 155 Menu 3.2 TCP/IP Setup .....                                     | 233 |
| Figure 156 Menu 23 System Password .....                                   | 235 |
| Figure 157 Menu 24 System Maintenance .....                                | 237 |
| Figure 158 Menu 24.1 System Maintenance: Status .....                      | 238 |
| Figure 159 Menu 24.2 System Information and Console Port Speed .....       | 239 |
| Figure 160 Menu 24.2.1 System Information: Information .....               | 239 |
| Figure 161 Menu 24.2.2 System Maintenance: Change Console Port Speed ..... | 240 |
| Figure 162 Menu 24.3 System Maintenance: Log and Trace .....               | 240 |
| Figure 163 Sample Error and Information Messages .....                     | 241 |
| Figure 164 Menu 24.4 System Maintenance: Diagnostic .....                  | 241 |
| Figure 165 FTP Session Example .....                                       | 245 |
| Figure 166 FTP Session Example .....                                       | 247 |
| Figure 167 Menu 24 System Maintenance .....                                | 249 |

|   |     |
|---|-----|
| Figure 168 Valid CI Commands .....  | 250 |
| Figure 169 Menu 24.10 System Maintenance: Time and Date Setting .....       | 251 |
| Figure 170 Menu 24.11 Remote Management Control .....                       | 253 |
| Figure 171 WIndows 95/98/Me: Network: Configuration .....                   | 270 |
| Figure 172 Windows 95/98/Me: TCP/IP Properties: IP Address .....            | 271 |
| Figure 173 Windows 95/98/Me: TCP/IP Properties: DNS Configuration .....     | 272 |
| Figure 174 Windows XP: Start Menu .....                                     | 273 |
| Figure 175 Windows XP: Control Panel .....                                  | 273 |
| Figure 176 Windows XP: Control Panel: Network Connections: Properties ..... | 274 |
| Figure 177 Windows XP: Local Area Connection Properties .....               | 274 |
| Figure 178 Windows XP: Advanced TCP/IP Settings .....                       | 275 |
| Figure 179 Windows XP: Internet Protocol (TCP/IP) Properties .....          | 276 |
| Figure 180 Macintosh OS 8/9: Apple Menu .....                               | 277 |
| Figure 181 Macintosh OS 8/9: TCP/IP .....                                   | 277 |
| Figure 182 Macintosh OS X: Apple Menu .....                                 | 278 |
| Figure 183 Macintosh OS X: Network .....                                    | 279 |
| Figure 184 Peer-to-Peer Communication in an Ad-hoc Network .....            | 281 |
| Figure 185 Basic Service Set .....  | 282 |
| Figure 186 Infrastructure WLAN .....  | 283 |
| Figure 187 RTS/CTS .....  | 284 |
| Figure 188 WPA(2) with RADIUS Application Example .....                     | 291 |
| Figure 189 WPA(2)-PSK Authentication .....                                  | 292 |
| Figure 190 Pop-up Blocker .....   | 295 |
| Figure 191 Internet Options: Privacy .....                                  | 296 |
| Figure 192 Internet Options: Privacy .....                                  | 297 |
| Figure 193 Pop-up Blocker Settings .....                                    | 297 |
| Figure 194 Internet Options: Security .....                                 | 298 |
| Figure 195 Security Settings - Java Scripting .....                         | 299 |
| Figure 196 Security Settings - Java .....                                   | 299 |
| Figure 197 Java (Sun) .....   | 300 |
| Figure 198 Network Number and Host ID .....                                 | 302 |
| Figure 199 Subnetting Example: Before Subnetting .....                      | 304 |
| Figure 200 Subnetting Example: After Subnetting .....                       | 305 |
| Figure 201 Text File Based Auto Configuration .....                         | 309 |
| Figure 202 Configuration File Format .....                                  | 311 |
| Figure 203 WEP Configuration File Example .....                             | 312 |
| Figure 204 802.1X Configuration File Example .....                          | 313 |
| Figure 205 WPA-PSK Configuration File Example .....                         | 313 |
| Figure 206 WPA Configuration File Example .....                             | 314 |
| Figure 207 Wlan Configuration File Example .....                            | 315 |



# List of Tables

|  |     |
|--|-----|
| Table 1 The Status Screen .....                                      | 45  |
| Table 2 Tutorial: Example Information .....                          | 53  |
| Table 3 Tutorial: Rogue AP Example Information .....                 | 63  |
| Table 4 Tutorial: Friendly AP Information .....                      | 65  |
| Table 5 Tutorial: SSID Profile Security Settings .....               | 70  |
| Table 6 Tutorial: Example Network MAC Addresses .....                | 71  |
| Table 7 Tutorial: Example User MAC Addresses .....                   | 71  |
| Table 8 Tutorial: SERVER_2 Network Information .....                 | 74  |
| Table 9 System > General .....                                       | 79  |
| Table 10 Password .....  | 81  |
| Table 11 SYSTEM > Time Setting .....                                 | 83  |
| Table 12 Default Time Servers .....                                  | 84  |
| Table 13 WMM QoS Priorities .....                                    | 87  |
| Table 14 Typical Packet Sizes .....                                  | 87  |
| Table 15 Automatic Traffic Classifier Priorities .....               | 87  |
| Table 16 ATC + WMM Priority Assignment (LAN to WLAN) .....           | 88  |
| Table 17 ATC + WMM Priority Assignment (WLAN to LAN) .....           | 88  |
| Table 18 ToS and IEEE 802.1d to WMM QoS Priority Level Mapping ..... | 90  |
| Table 19 STP Path Costs .....  | 90  |
| Table 20 STP Port States .....                                       | 91  |
| Table 21 Wireless: Access Point .....                                | 93  |
| Table 22 Wireless: Bridge/Repeater .....                             | 96  |
| Table 23 Types of Encryption for Each Type of Authentication .....   | 102 |
| Table 24 Security Modes .....  | 103 |
| Table 25 WIRELESS > Security .....                                   | 104 |
| Table 26 Security: WEP .....   | 105 |
| Table 27 Security: 802.1x Only .....                                 | 106 |
| Table 28 Security: 802.1x Static 64-bit, 802.1x Static 128-bit ..... | 107 |
| Table 29 Security: WPA .....   | 108 |
| Table 30 Security: WPA2 or WPA2-MIX .....                            | 109 |
| Table 31 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX .....           | 110 |
| Table 32 RADIUS .....  | 112 |
| Table 33 Wireless: Multiple BSS .....                                | 115 |
| Table 34 SSID .....  | 118 |
| Table 35 Configuring SSID .....                                      | 119 |
| Table 36 WIRELESS > Layer-2 Isolation .....                          | 123 |
| Table 37 WIRELESS > Layer-2 Isolation Configuration .....            | 124 |
| Table 38 WIRELESS > MAC Filter .....                                 | 127 |

|  |     |
|--|-----|
| Table 39 MAC Address Filter .....  | 128 |
| Table 40 Private IP Address Ranges .....                                 | 133 |
| Table 41 IP Setup .....  | 134 |
| Table 42 ROGUE AP > Configuration .....                                  | 140 |
| Table 43 ROGUE AP > Friendly AP .....                                    | 141 |
| Table 44 ROGUE AP > Rogue AP .....                                       | 142 |
| Table 45 Remote Management Overview .....                                | 143 |
| Table 46 Remote Management: Telnet .....                                 | 146 |
| Table 47 Remote Management: FTP .....                                    | 147 |
| Table 48 Remote Management: WWW .....                                    | 149 |
| Table 49 SNMP Traps .....  | 156 |
| Table 50 SNMP Interface Index to Physical and Virtual Port Mapping ..... | 157 |
| Table 51 Remote Management: SNMP .....                                   | 158 |
| Table 52 Remote Management: SNMP User Profile .....                      | 159 |
| Table 53 Internal RADIUS Server Setting Screen Setting .....             | 162 |
| Table 54 Trusted AP .....  | 165 |
| Table 55 Trusted Users .....   | 166 |
| Table 56 My Certificates .....   | 172 |
| Table 57 My Certificate Import .....                                     | 175 |
| Table 58 My Certificate Create .....                                     | 176 |
| Table 59 My Certificate Details .....                                    | 178 |
| Table 60 Trusted CAs .....   | 181 |
| Table 61 Trusted CA Import .....   | 182 |
| Table 62 Trusted CA Details .....  | 183 |
| Table 63 View Log .....  | 187 |
| Table 64 Log Settings .....  | 189 |
| Table 65 System Maintenance Logs .....                                   | 190 |
| Table 66 ICMP Notes .....  | 191 |
| Table 67 Sys log .....   | 192 |
| Table 68 Log Categories and Available Settings Example .....             | 192 |
| Table 69 Wireless VLAN .....   | 197 |
| Table 70 RADIUS VLAN .....   | 199 |
| Table 71 Standard RADIUS Attributes .....                                | 202 |
| Table 72 System Status .....   | 213 |
| Table 73 System Status: Show Statistics .....                            | 215 |
| Table 74 Association List .....  | 216 |
| Table 75 Channel Usage .....   | 217 |
| Table 76 Firmware Upload .....   | 218 |
| Table 77 Restore Configuration .....                                     | 220 |
| Table 78 SMT Menus Overview .....  | 228 |
| Table 79 Main Menu Commands .....  | 229 |
| Table 80 Main Menu Summary .....   | 230 |
| Table 81 Menu 1 General Setup .....                                      | 231 |

|  |     |
|--|-----|
| Table 82 Menu 3.2 TCP/IP Setup .....                                   | 234 |
| Table 83 Menu 24.1 System Maintenance: Status .....                    | 238 |
| Table 84 Menu 24.2.1 System Maintenance: Information .....             | 239 |
| Table 85 Menu 24.4 System Maintenance Menu: Diagnostic .....           | 242 |
| Table 86 Filename Conventions .....                                    | 244 |
| Table 87 General Commands for Third Party FTP Clients .....            | 245 |
| Table 88 General Commands for Third Party TFTP Clients .....           | 246 |
| Table 89 Brute-Force Password Guessing Protection Commands .....       | 250 |
| Table 90 System Maintenance: Time and Date Setting .....               | 251 |
| Table 91 Menu 24.11 Remote Management Control .....                    | 254 |
| Table 92 Hardware Specifications .....                                 | 261 |
| Table 93 Firmware Specifications .....                                 | 262 |
| Table 94 ZyXEL Device Compatible Antennas .....                        | 264 |
| Table 95 ZyXEL Device Compatible Antenna Cables .....                  | 264 |
| Table 96 Power over Ethernet Injector Specifications .....             | 265 |
| Table 97 Power over Ethernet Injector RJ-45 Port Pin Assignments ..... | 265 |
| Table 98 IEEE 802.11g .....  | 285 |
| Table 99 Wireless Security Levels .....                                | 286 |
| Table 100 Comparison of EAP Authentication Types .....                 | 289 |
| Table 101 Wireless Security Relational Matrix .....                    | 292 |
| Table 102 Subnet Masks .....   | 302 |
| Table 103 Subnet Masks .....   | 303 |
| Table 104 Maximum Host Numbers .....                                   | 303 |
| Table 105 Alternative Subnet Mask Notation .....                       | 303 |
| Table 106 Subnet 1 .....   | 305 |
| Table 107 Subnet 2 .....   | 306 |
| Table 108 Subnet 3 .....   | 306 |
| Table 109 Subnet 4 .....   | 306 |
| Table 110 Eight Subnets .....  | 306 |
| Table 111 24-bit Network Number Subnet Planning .....                  | 307 |
| Table 112 16-bit Network Number Subnet Planning .....                  | 307 |
| Table 113 Auto Configuration by DHCP .....                             | 310 |
| Table 114 Manual Configuration .....                                   | 310 |
| Table 115 Configuration via SNMP .....                                 | 311 |
| Table 116 Displaying the File Version .....                            | 311 |
| Table 117 Displaying the File Version .....                            | 311 |
| Table 118 Displaying the Auto Configuration Status .....               | 312 |



---

# PART I

# Introduction

---

Introducing the ZyXEL Device (33)

Introducing the Web Configurator (41)

Status Screens (45)

Tutorial (49)



# Introducing the ZyXEL Device

This chapter introduces the main applications and features of the ZyXEL Device. It also introduces the ways you can manage the ZyXEL Device.

## 1.1 Introducing the ZyXEL Device

Your ZyXEL Device extends the range of your existing wired network without additional wiring, providing easy network access to mobile users.

It is highly versatile, supporting multiple BSSIDs simultaneously. The Quality of Service (QoS) features allow you to prioritize time-sensitive or highly important applications such as VoIP.

Multiple security profiles allow you to easily assign different types of security to groups of users. The ZyXEL Device controls network access with MAC address filtering, rogue AP detection, layer 2 isolation and an internal authentication server. It also provides a high level of network traffic security, supporting IEEE 802.1x, Wi-Fi Protected Access (WPA), WPA2 and WEP data encryption.

Your ZyXEL Device is easy to install, configure and use. The embedded Web-based configurator enables simple, straightforward management and maintenance.

See the Quick Start Guide for instructions on how to make hardware connections.

## 1.2 Applications for the ZyXEL Device

The ZyXEL Device can be configured to use the following WLAN operating modes

- 1 Access Point (AP)
- 2 Bridge/Repeater
- 3 AP+Bridge
- 4 MBSSID

Applications for each operating mode are shown below.



---

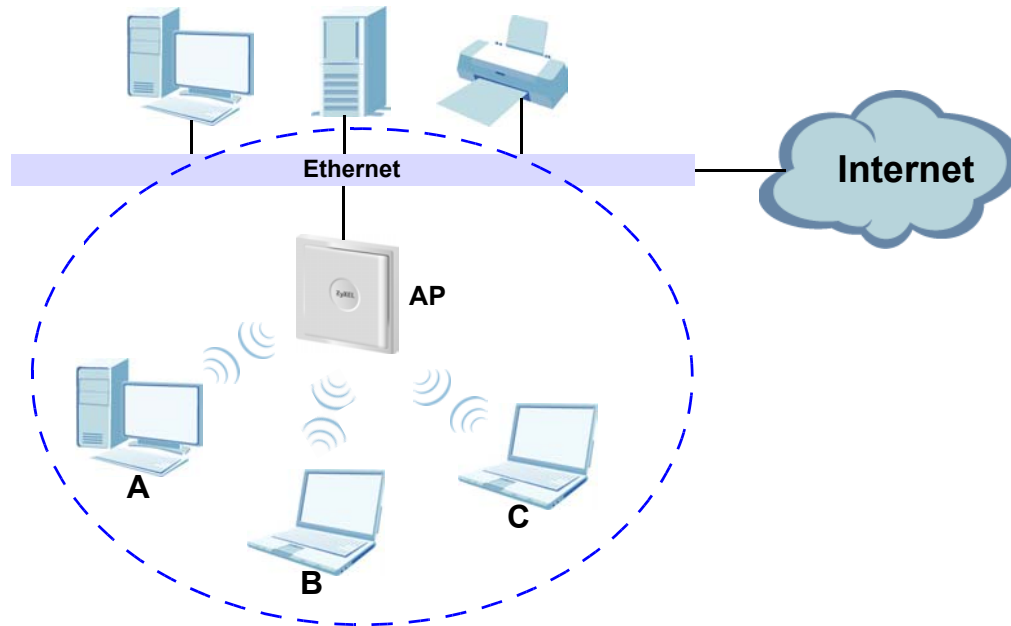
A different channel should be configured for each WLAN interface to reduce the effects of radio interference.

---

## 1.2.1 Access Point

The ZyXEL Device is an ideal access solution for wireless Internet connection. A typical Internet access application for your ZyXEL Device is shown as follows. Clients **A**, **B** and **C** can access the wired network through the ZyXEL Devices.

**Figure 1** Access Point Application



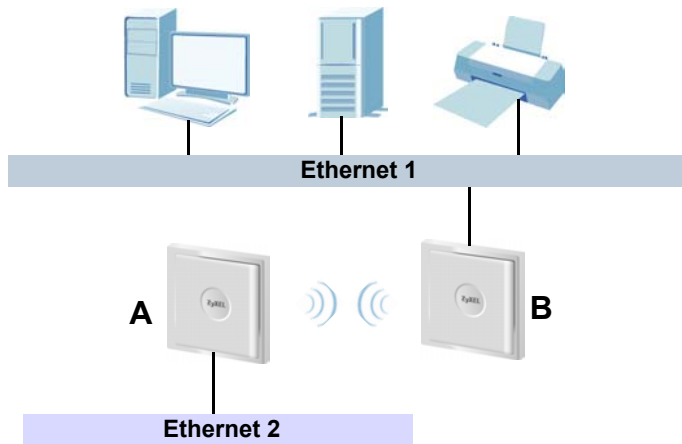
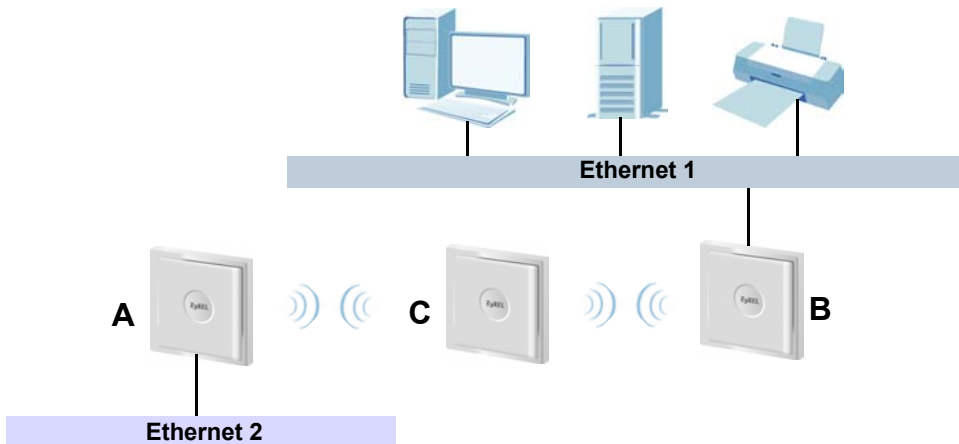
## 1.2.2 Bridge / Repeater

The ZyXEL Device can act as a wireless network bridge and establish wireless links with other APs. In the figure below, the two ZyXEL Devices (**A** and **B**) are connected to independent wired networks and have a bridge connection (**A** can communicate with **B**) at the same time. A ZyXEL Device in repeater mode (**C**) has no Ethernet connection. When the ZyXEL Device is in bridge mode, you should enable STP to prevent bridge loops.

When the ZyXEL Device is in **Bridge / Repeater** mode, security between APs (the Wireless Distribution System or WDS) is independent of the security between the wireless stations and the AP. If you do not enable WDS security, traffic between APs is not encrypted. When WDS security is enabled, both APs must use the same pre-shared key. See [Section 6.7.2 on page 94](#) for more details.

Once the security settings of peer sides match one another, the connection between devices is made.

At the time of writing, WDS security is compatible with other ZyXEL access points only. Refer to your other access point's documentation for details.

**Figure 2** Bridge Application**Figure 3** Repeater Application

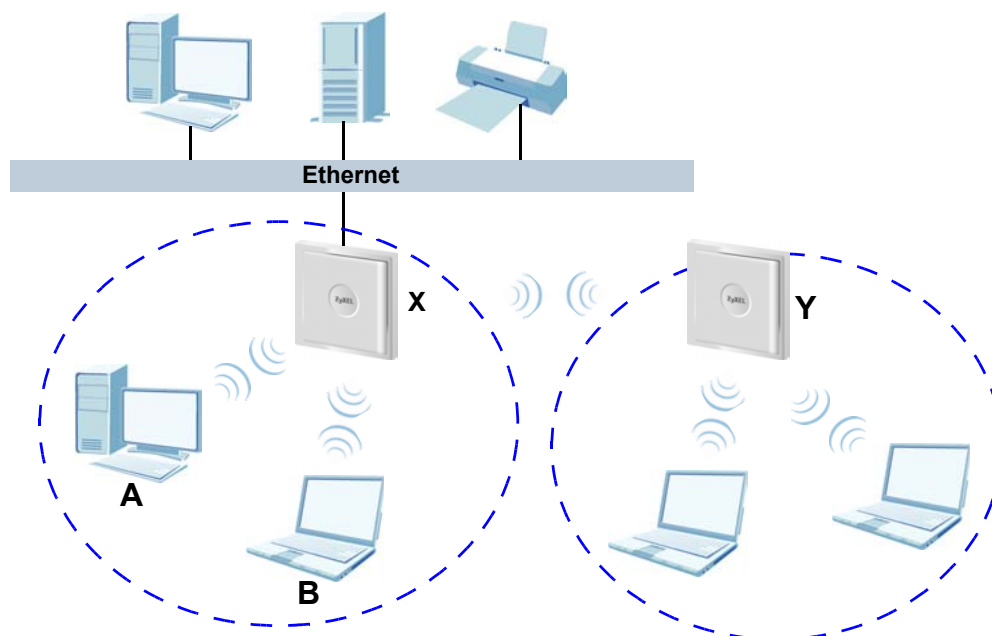
### 1.2.3 AP + Bridge

In **AP+Bridge** mode, the ZyXEL Device supports both AP and bridge connection at the same time.

In the figure below, **A** and **B** use **X** as an **AP** to access the wired network, while **X** and **Y** communicate in bridge mode.

When the ZyXEL Device is in **AP + Bridge** mode, security between APs (the Wireless Distribution System or WDS) is independent of the security between the wireless stations and the AP. If you do not enable WDS security, traffic between APs is not encrypted. When WDS security is enabled, both APs must use the same pre-shared key. See [Section 6.7.3 on page 98](#) for more details.

Unless specified, the term “security settings” refers to the traffic between the wireless stations and the ZyXEL Device.

**Figure 4** AP+Bridge Application

### 1.2.4 MBSSID

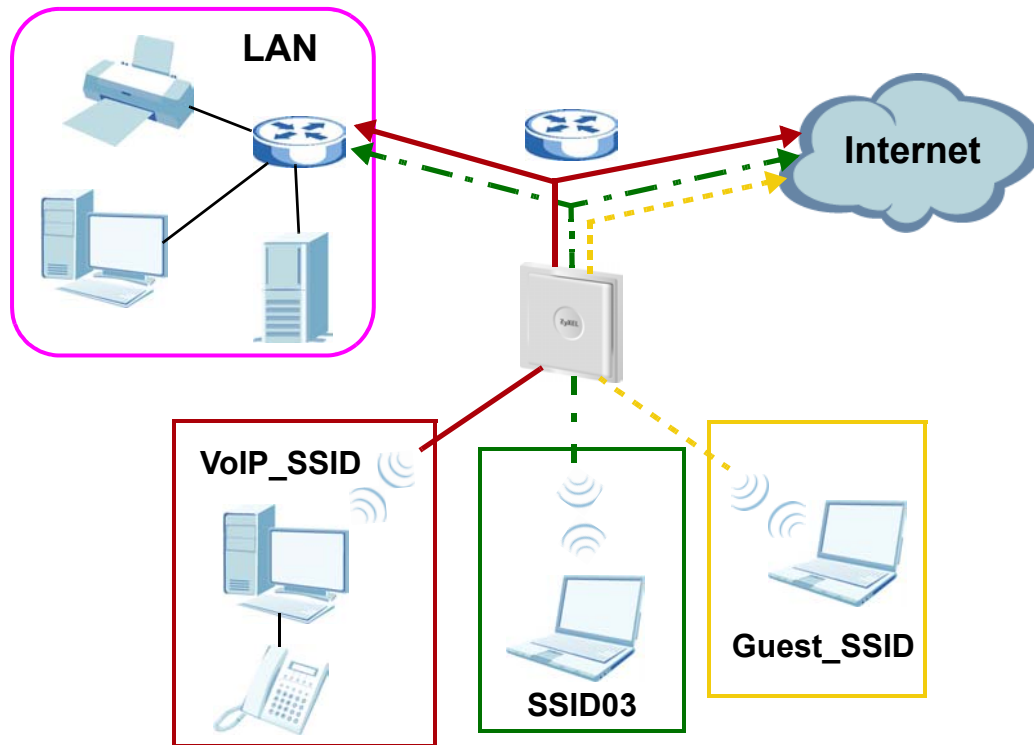
A BSS (Basic Service Set) is the set of devices forming a single wireless network (usually an access point and one or more wireless clients). An SSID (Service Set Identifier) is the name of a BSS. In MBSSID (Multiple BSS) mode, the ZyXEL Device provides multiple virtual APs, each forming its own BSS and using its own individual SSID profile.

You can configure up to sixteen SSID profiles, and have up to eight active at any one time.

You can assign different wireless and security settings to each SSID profile. This allows you to compartmentalize groups of users, set varying access privileges, and prioritize network traffic to and from certain BSSs.

To the wireless clients in the network, each SSID appears to be a different access point. As in any wireless network, clients can associate only with the SSIDs for which they have the correct security settings.

For example, you might want to set up a wireless network in your office where Internet telephony (Voice over IP, or VoIP) users have priority. You also want a regular wireless network for standard users, as well as a 'guest' wireless network for visitors. In the following figure, **VoIP\_SSID** users have Quality of Service (QoS) priority, **SSID03** is the wireless network for standard users, and **Guest\_SSID** is the wireless network for guest users. In this example, the guest user is forbidden access to the wired LAN behind the AP and can access only the Internet.

**Figure 5** Multiple BSSs

### 1.2.5 Pre-Configured SSID Profiles

The ZyXEL Device has two pre-configured SSID profiles.

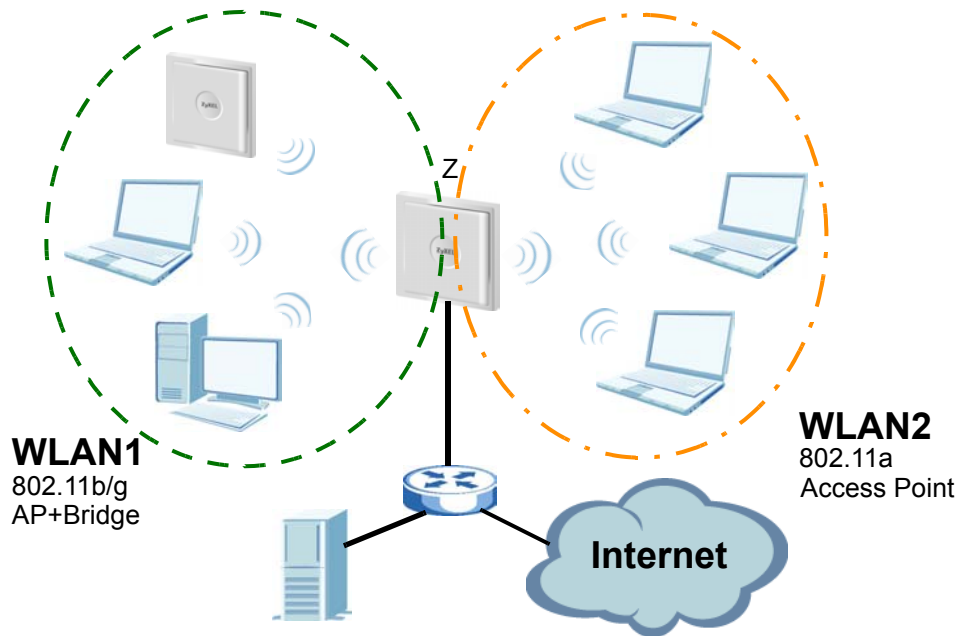
- 1 VoIP\_SSID.** This profile is intended for use by wireless clients requiring the highest QoS (Quality of Service) level for VoIP (Voice over IP) telephony and other applications requiring low latency. The QoS level of this profile is not user-configurable. See [Chapter 6 on page 85](#) for more information on QoS.
- 2 Guest\_SSID.** This profile is intended for use by visitors and others who require access to certain resources on the network (an Internet gateway or a network printer, for example) but must not have access to the rest of the network. Layer 2 isolation is enabled (see [Section 9.1 on page 121](#)), and QoS is set to **NONE**. Intra-BSS traffic blocking is also enabled (see [Section 8.2 on page 117](#)). These fields are all user-configurable.

### 1.2.6 Configuring Dual WLAN Adaptors

The ZyXEL Device is equipped with dual wireless adaptors. This means you can configure two different wireless networks to operate simultaneously.

In the following example, the ZyXEL Device (**Z**) uses **WLAN1** in **AP+Bridge** mode to allow IEEE 802.11b/g APs and clients to communicate with the wired network, and **WLAN2** in **Access Point** mode to allow IEEE 802.11a clients to access the wired network.

**Figure 6** Dual WLAN Adaptors Example



## 1.3 Ways to Manage the ZyXEL Device

Use any of the following methods to manage the ZyXEL Device.

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- SMT. System Management Terminal is a text-based configuration menu that you can use to configure your device. Use Telnet to access the SMT.
- FTP for firmware upgrades and configuration backup and restore.
- SNMP. The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.

## 1.4 Configuring Your ZyXEL Device's Security Features

Your ZyXEL Device comes with a variety of security features. This section summarizes these features and provides links to sections in the User's Guide to configure security settings on your ZyXEL Device. Follow the suggestions below to improve security on your ZyXEL Device and network.

### 1.4.1 Control Access to Your Device

Ensure only people with permission can access your ZyXEL Device.

- Control physical access by locating devices in secure areas, such as locked rooms. Most ZyXEL Devices have a reset button. If an unauthorized person has access to the reset button, they can then reset the device's password to its default password, log in and reconfigure its settings.
- Change any default passwords on the ZyXEL Device, such as the password used for accessing the ZyXEL Device's web configurator (if it has a web configurator). Use a password with a combination of letters and numbers and change your password regularly. Write down the password and put it in a safe place.
- Avoid setting a long timeout period before the ZyXEL Device's web configurator automatically times out. A short timeout reduces the risk of unauthorized person accessing the web configurator while it is left idle.

See [Chapter 5 on page 79](#) for instructions on changing your password and setting the timeout period.

- Configure remote management to control who can manage your ZyXEL Device. See [Chapter 12 on page 143](#) for more information. If you enable remote management, ensure you have enabled remote management only on the IP addresses, services or interfaces you intended and that other remote management settings are disabled.

### 1.4.2 Wireless Security

Wireless devices are especially vulnerable to attack. If your ZyXEL Device has a wireless function, take the following measures to improve wireless security.

- Enable wireless security on your ZyXEL Device. Choose the most secure encryption method that all devices on your network support. See [Section 7.3 on page 103](#) for directions on configuring encryption. If you have a RADIUS server, enable IEEE 802.1x or WPA(2) user identification on your network so users must log in. This method is more common in business environments.
- Hide your wireless network name (SSID). The SSID can be regularly broadcast and unauthorized users may use this information to access your network. See [Section 8.2 on page 117](#) for directions on using the web configurator to hide the SSID.
- Enable the MAC filter to allow only trusted users to access your wireless network or deny unwanted users access based on their MAC address. See [Section 9.4 on page 126](#) for directions on configuring the MAC filter.

## 1.5 Maintaining Your ZyXEL Device

Do the following things regularly to keep your ZyXEL Device running.

- Check the ZyXEL website ([www.zyxel.com.tw](http://www.zyxel.com.tw)) regularly for new firmware for your ZyXEL Device. Ensure you download the correct firmware for your model.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the ZyXEL Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the ZyXEL Device. You could simply restore your last configuration.

## 1.6 Hardware Connections

See your Quick Start Guide for information on making hardware connections.



---

Your ZyXEL Device has two wireless LAN adaptors, WLAN1 and WLAN2. WLAN1 uses the **RF1** antenna and WLAN2 uses the **RF2** antenna. If you connect only one antenna, you can use only the associated wireless LAN adaptor.

---

# Introducing the Web Configurator

This chapter describes how to access the ZyXEL Device's web configurator and provides an overview of its screens.

## 2.1 Accessing the Web Configurator

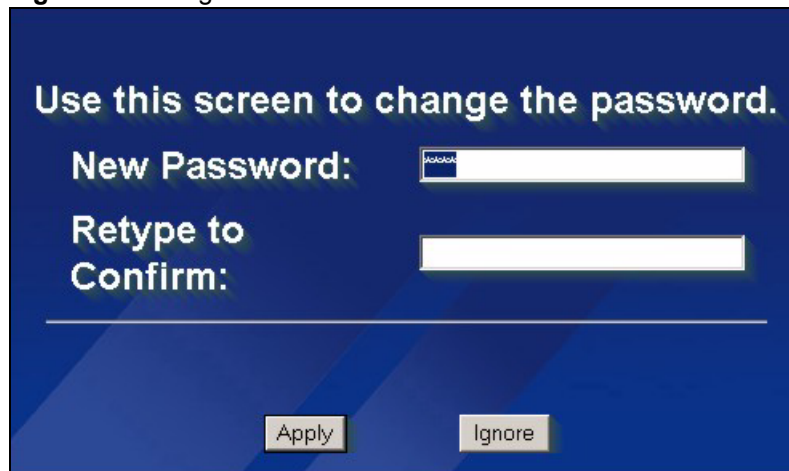
- 1 Make sure your hardware is properly connected and prepare your computer or computer network to connect to the ZyXEL Device (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "192.168.1.2" as the URL (default).
- 4 Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.
- 5 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) then click **Apply**. Alternatively, click **Ignore**.



---

If you do not change the password, the following screen appears every time you login.

---


**Figure 7** Change Password Screen


Use this screen to change the password.

New Password:

Retype to Confirm:

- 6** Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyXEL Device's MAC address that will be specific to this device.

**Figure 8** Replace Certificate Screen


**Replace Factory Default Certificate**

The factory default certificate is common to all NWA models. Click Apply to create a certificate using your NWA's MAC address that will be specific to this device.

You should now see the **Status** screen. See [Chapter 2 on page 41](#) for details about the **Status** screen.



The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the ZyXEL Device if this happens.

## 2.2 Resetting the ZyXEL Device

This replaces the current configuration file with the factory-default configuration file. This means that you will lose all the settings you previously configured. The password will be reset to 1234.

## 2.2.1 Methods of Restoring Factory-Defaults

You can erase the current configuration and restore factory defaults in the following ways:

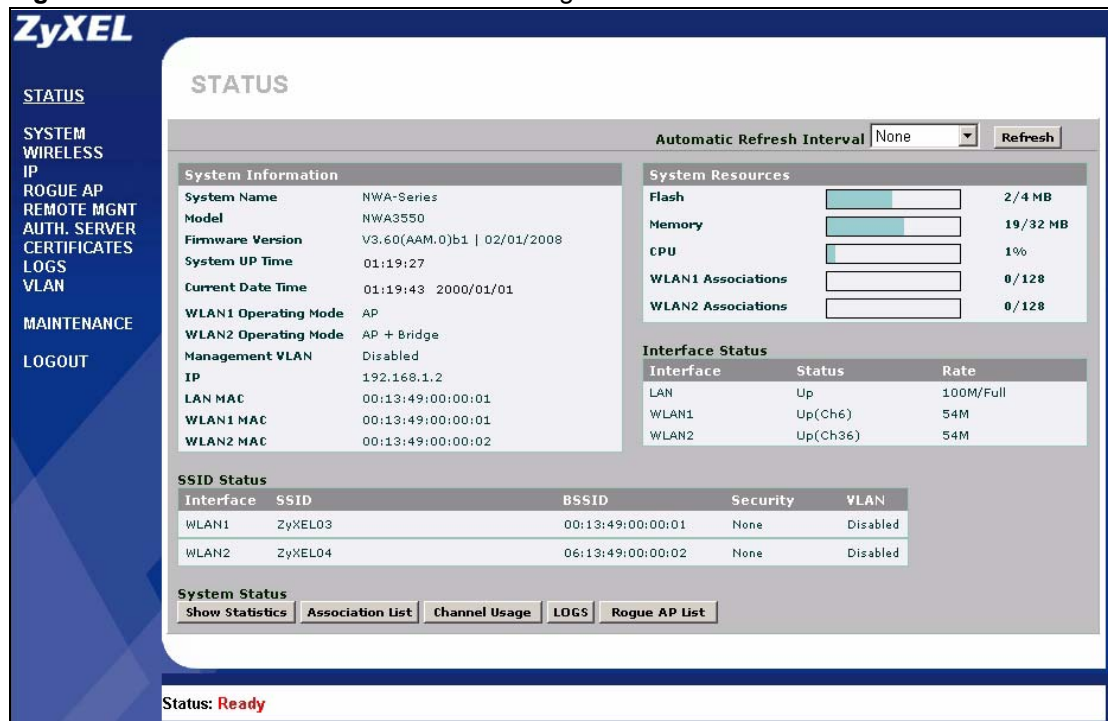
- Use the web configurator to restore defaults (refer to [Chapter 17 on page 213](#)).
- Transfer the configuration file to your ZyXEL Device using FTP. See the section on SMT configuration for more information.

## 2.3 Navigating the Web Configurator

The following summarizes how to navigate the web configurator from the **Status** screen.

- Click **LOGOUT** at any time to exit the web configurator.
- Check the status bar at the bottom of the screen when you click **Apply** or **OK** to verify that the configuration has been updated.

**Figure 9** The Status Screen of the Web Configurator



- Click the links on the left of the screen to configure advanced features such as **SYSTEM** (General, Password and Time Setting), **WIRELESS** (Wireless, SSID, Security, RADIUS, Layer-2 Isolation, MAC Filter), **IP**, **ROGUE AP** (Configuration, Friendly AP, Rogue AP), **REMOTE MGNT** (Telnet, FTP, WWW and SNMP), **AUTH. SERVER** (Setting, Trusted AP, Trusted Users), **CERTIFICATES** (My Certificates, Trusted CAs), **LOGS** (View Log and Log Settings) and **VLAN** (Wireless VLAN and RADIUS VLAN).
- Click **MAINTENANCE** to view information about your ZyXEL Device or upgrade configuration and firmware files. Maintenance features include **Status** (Statistics), **Association List**, **Channel Usage**, **F/W** (firmware) **Upload**, **Configuration** (Backup, Restore and Default) and **Restart**.



# Status Screens

The **Status** screen displays when you log into the ZyXEL Device, or click **STATUS** in the navigation menu.

Use the **Status** screens to look at the current status of the device, system resources, interfaces and SSID status. The **Status** screen also provides detailed information about associated wireless clients, channel usage, logs and detected rogue APs.

## 3.1 The Status Screen

Click **Status**. The following screen displays.

**Figure 10** The Status Screen

The screenshot shows the 'STATUS' screen of a ZyXEL device. At the top right, there is an 'Automatic Refresh Interval' dropdown set to 'None' and a 'Refresh' button. The main content is divided into four sections:

- System Information:** A table with fields like System Name (NWA-Series), Model (NWA3550), Firmware Version (V3.60(AAM.0)b1 | 02/01/2008), System UP Time (01:19:27), Current Date Time (01:19:43 2000/01/01), WLAN1 Operating Mode (AP), WLAN2 Operating Mode (AP + Bridge), Management VLAN (Disabled), IP (192.168.1.2), LAN MAC (00:13:49:00:00:01), WLAN1 MAC (00:13:49:00:00:01), and WLAN2 MAC (00:13:49:00:00:02).
- System Resources:** A section with progress bars and values for Flash (2/4 MB), Memory (19/32 MB), CPU (1%), WLAN1 Associations (0/128), and WLAN2 Associations (0/128).
- Interface Status:** A table with columns Interface, Status, and Rate. It shows LAN (Up, 100M/Full), WLAN1 (Up(Ch6), 54M), and WLAN2 (Up(Ch36), 54M).
- SSID Status:** A table with columns Interface, SSID, BSSID, Security, and VLAN. It shows WLAN1 (ZyXEL03, 00:13:49:00:00:01, None, Disabled) and WLAN2 (ZyXEL04, 06:13:49:00:00:02, None, Disabled).

At the bottom, there is a 'System Status' section with buttons for 'Show Statistics', 'Association List', 'Channel Usage', 'LOGS', and 'Rogue AP List'.

The following table describes the labels in this screen.

**Table 1** The Status Screen

| LABEL                      | DESCRIPTION  |
|----------------------------|--|
| Automatic Refresh Interval | Enter how often you want the ZyXEL Device to update this screen. |
| Refresh                    | Click this to update this screen immediately.                    |

**Table 1** The Status Screen

| <b>LABEL</b>         | <b>DESCRIPTION</b>   |
|----------------------|--|
| System Information   |  |
| System Name          | This field displays the ZyXEL Device system name. It is used for identification. You can change this in the <b>System &gt; General</b> screen's <b>System Name</b> field.  |
| Model                | This field displays the ZyXEL Device's exact model name.   |
| Firmware Version     | This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. You can change the firmware version by uploading new firmware in <b>Maintenance &gt; F/W Upload</b> .  |
| System Up Time       | This field displays the elapsed time since the ZyXEL Device was turned on.   |
| Current Date Time    | This field displays the date and time configured on the ZyXEL Device. You can change this in the <b>System &gt; Time Setting</b> screen.   |
| WLAN1 Operating Mode | This field displays the current operating mode of the first wireless module ( <b>AP, Bridge / Repeater, AP + Bridge</b> or <b>MBSSID</b> ). You can change the operating mode in the <b>Wireless &gt; Wireless</b> screen.   |
| WLAN2 Operating Mode | This field displays the current operating mode of the second wireless module ( <b>AP, Bridge / Repeater, AP + Bridge</b> or <b>MBSSID</b> ). You can change the operating mode in the <b>Wireless &gt; Wireless</b> screen.  |
| Management VLAN      | This field displays the management VLAN ID if VLAN is active, or <b>Disabled</b> if it is not active. You can enable or disable VLAN, or change the management VLAN ID, in the <b>VLAN &gt; Wireless VLAN</b> screen.  |
| IP                   | This field displays the current IP address of the ZyXEL Device on the network.   |
| LAN MAC              | This displays the MAC (Media Access Control) address of the ZyXEL Device on the LAN. Every network device has a unique MAC address which identifies it across the network. Your ZyXEL Device features dual wireless module, and has two MAC addresses. The MAC address of the first wireless module ( <b>WLAN1</b> ) is used on the LAN. |
| WLAN1 MAC            | This displays the MAC address of the first wireless module.  |
| WLAN2 MAC            | This displays the MAC address of the second wireless module.   |
| System Resources     |  |
| Flash                | This field displays the amount of the ZyXEL Device's flash memory currently in use. The flash memory is used to store firmware and SSID profiles.  |
| Memory               | This field displays what percentage of the ZyXEL Device's volatile memory is currently in use. The higher the memory usage, the more likely the ZyXEL Device is to slow down. Some memory is required just to start the ZyXEL Device and to run the web configurator.  |
| CPU                  | This field displays what percentage of the ZyXEL Device's processing ability is currently being used. The higher the CPU usage, the more likely the ZyXEL Device is to slow down.  |
| WLAN1 Associations   | This field displays the number of wireless clients currently associated with the first wireless module. Each wireless module supports up to 128 concurrent associations.   |
| WLAN2 Associations   | This field displays the number of wireless clients currently associated with the second wireless module. Each wireless module supports up to 128 concurrent associations.  |
| Interface Status     |  |
| Interface            | This column displays each interface of the ZyXEL Device.   |

**Table 1** The Status Screen

| <b>LABEL</b>     | <b>DESCRIPTION</b>  |
|------------------|---|
| Status           | This field indicates whether or not the ZyXEL Device is using the interface. For each interface, this field displays <b>Up</b> when the ZyXEL Device is using the interface and <b>Down</b> when the ZyXEL Device is not using the interface. |
| Rate             | For the LAN port this displays the port speed and duplex setting. For the WLAN1 and WLAN2 interfaces, it displays the downstream and upstream transmission rate or <b>N/A</b> if the interface is not in use.                                 |
| SSID Status      |   |
| Interface        | This column displays each of the ZyXEL Device's wireless interfaces, <b>WLAN1</b> and <b>WLAN2</b> .  |
| SSID             | This field displays the SSID(s) currently used by each wireless module.   |
| BSSID            | This field displays the MAC address of the wireless adaptor.  |
| Security         | This field displays the type of wireless security used by each SSID.  |
| VLAN             | This field displays the VLAN ID of each SSID in use, or <b>Disabled</b> if the SSID does not use VLAN.  |
| System Status    |   |
| Show Statistics  | Click this link to view port status and packet specific statistics. See <a href="#">Section 17.2.1 on page 214</a> .  |
| Association List | Click this to see a list of wireless clients currently associated to each of the ZyXEL Device's wireless modules. See <a href="#">Section 17.3 on page 215</a> .  |
| Channel Usage    | Click this to see which wireless channels are currently in use in the local area. See <a href="#">Section 17.4 on page 216</a> .  |
| Logs             | Click this to see a list of logs produced by the ZyXEL Device. See <a href="#">Section 15.1 on page 187</a> .   |
| Rogue AP List    | Click this to see a list of unauthorized access points in the local area. See <a href="#">Section 11.3.3 on page 141</a> .  |



# Tutorial

This chapter first provides an overview of how to configure the wireless LAN on your ZyXEL Device, and then gives step-by-step guidelines showing how to configure your ZyXEL Device for some example scenarios.

## 4.1 How to Configure the Wireless LAN

This section shows how to choose which wireless operating mode you should use on the ZyXEL Device, and the steps you should take to set up the wireless LAN in each wireless mode. See [Section 4.1.3 on page 52](#) for links to more information on each step.

### 4.1.1 Choosing the Wireless Mode

- Use **Access Point** operating mode if you want to allow wireless clients to access your wired network, all using the same security and Quality of Service (QoS) settings. See [Section 1.2.1 on page 34](#) for details.
- Use **Bridge/Repeater** operating mode if you want to use the ZyXEL Device to communicate with other access points. See [Section 1.2.2 on page 34](#) for details.  
The ZyXEL Device is a bridge when other APs access your wired Ethernet network through the ZyXEL Device.  
The ZyXEL Device is a repeater when it has no Ethernet connection and allows other APs to communicate with one another through the ZyXEL Device.
- Use **AP+Bridge** operating mode if you want to use the ZyXEL Device as an access point (see above) while also communicating with other access points. See [Section 1.2.3 on page 35](#) for details.
- Use **MBSSID** operating mode if you want to use the ZyXEL Device as an access point with some groups of users having different security or QoS settings from other groups of users. See [Section 1.2.4 on page 36](#) for details.

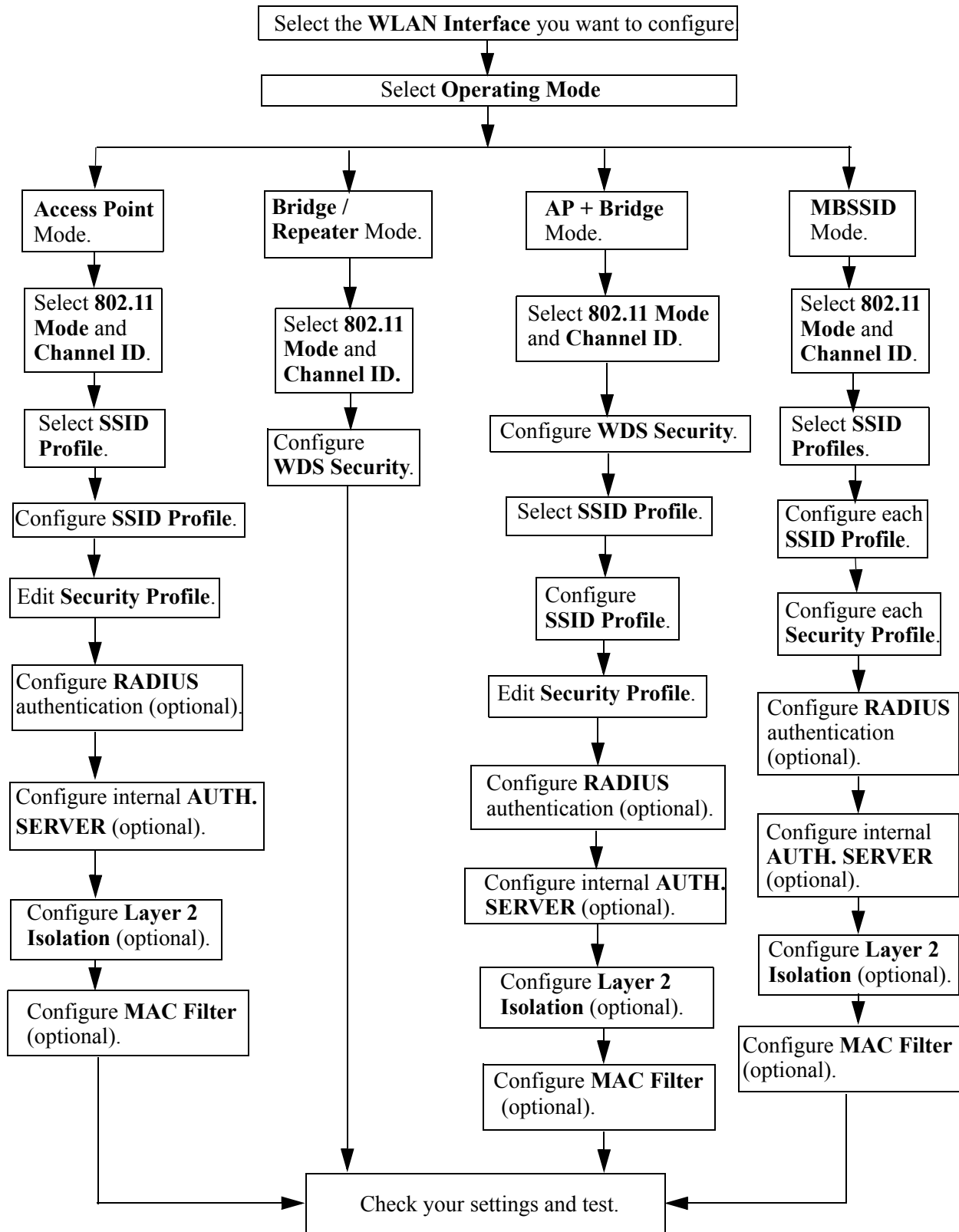
#### 4.1.1.1 Configuring Dual WLAN Adaptors

The ZyXEL Device is equipped with dual wireless adaptors. This means you can configure two different wireless networks to operate simultaneously. See [Section 1.2.6 on page 37](#) for details.

You can configure each wireless adaptor separately in the **WIRELESS > Wireless** screen. To configure the first wireless network, select **WLAN1** in the **WLAN Interface** field and follow the steps in [Section 4.1.2 on page 50](#). Then, select **WLAN2** in the **WLAN Interface** field and follow the same procedure to configure the second network.

### **4.1.2 Wireless LAN Configuration Overview**

The following figure shows the steps you should take to configure the wireless settings according to the operating mode you select. Use the Web Configurator to set up your ZyXEL Device's wireless network (see your Quick Start Guide for information on setting up your ZyXEL Device and accessing the Web Configurator).

**Figure 11** Configuring Wireless LAN

### 4.1.3 Further Reading

Use these links to find more information on the steps:

- Choosing **802.11 Mode**: see [Section 6.7.1 on page 92](#).
- Choosing a wireless **Channel ID**: see [Section 6.7.1 on page 92](#).
- Selecting and configuring **SSID profile(s)**: see [Section 6.7.1 on page 92](#) and [Section 8.2.1 on page 117](#).
- Configuring and activating **WDS Security**: see [Section 6.7.2 on page 94](#).
- Editing **Security Profile(s)**: see [Section 7.3 on page 103](#).
- Configuring an external **RADIUS** server: see [Section 7.5 on page 111](#).
- Configuring and activating the internal **AUTH. SERVER**: see [Section 7.4 on page 111](#) and [Chapter 13 on page 161](#).
- Configuring **Layer 2 Isolation**: see [Section 9.3 on page 123](#).
- Configuring **MAC Filtering**: see [Section 9.4 on page 126](#).

## 4.2 How to Configure Multiple Wireless Networks

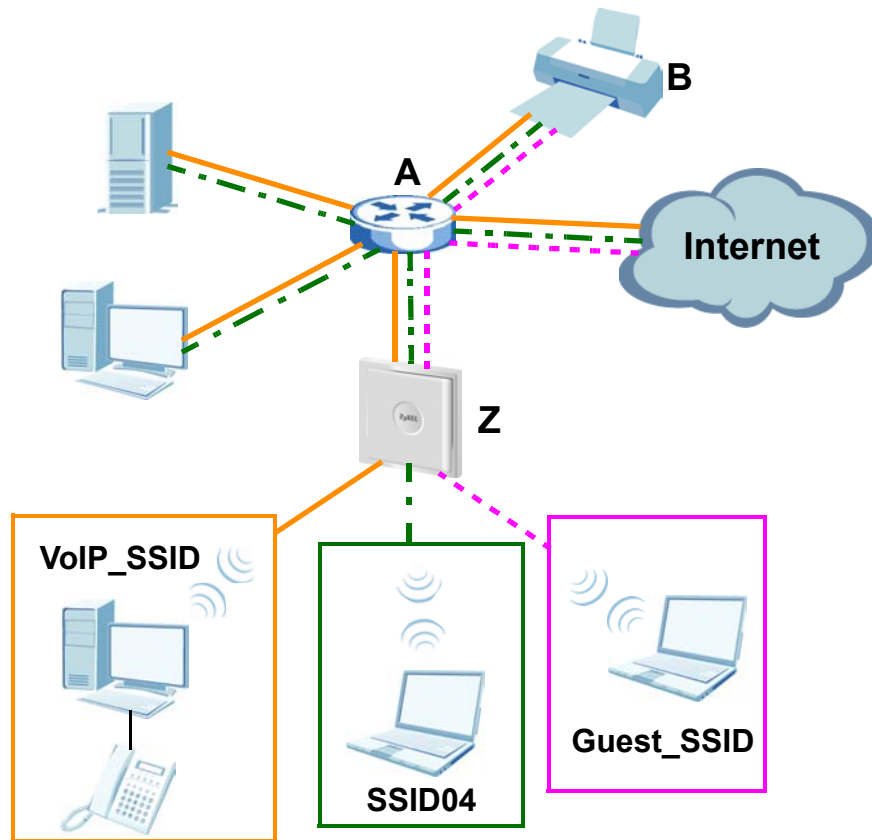
In this example, you have been using your ZyXEL Device as an access point for your office network (See your Quick Start Guide for information on how to set up your ZyXEL Device in Access Point mode). Now your network is expanding and you want to make use of the MBSSID feature (see [Section 8.1 on page 113](#)) to provide multiple wireless networks. Each wireless network will cater for a different type of user.

You want to make three wireless networks: one standard office wireless network with all the same settings you already have, another wireless network with high Quality of Service (QoS) settings for Voice over IP users, and a guest network that allows visitors to your office to access only the Internet and the network printer.

To do this, you will take the following steps:

- 1** Change the operating mode from Access Point to MBSSID and reactivate the standard network.
- 2** Configure a wireless network for Voice over IP users.
- 3** Configure a wireless network for guests to your office.

The following figure shows the multiple networks you want to set up. Your ZyXEL Device is marked **Z**, the main network router is marked **A**, and your network printer is marked **B**.

**Figure 12** Tutorial: Example MBSSID Setup

The standard network (**SSID04**) has access to all resources. The VoIP network (**VoIP\_SSID**) has access to all resources and a high Quality of Service (QoS) setting (see [Chapter 6 on page 85](#) for information on QoS). The guest network (**Guest\_SSID**) has access to the Internet and the network printer only, and a low QoS setting.

To configure these settings, you need to know the MAC (Media Access Control) addresses of the devices you want to allow users of the guest network to access. The following table shows the addresses used in this example.

**Table 2** Tutorial: Example Information

|  |                   |
|--|-------------------|
| Network router ( <b>A</b> ) MAC address  | 00:AA:00:AA:00:AA |
| Network printer ( <b>B</b> ) MAC address | AA:00:AA:00:AA:00 |

### 4.2.1 Change the Operating Mode

Log in to the ZyXEL Device (see [Section 2.1 on page 41](#)). Click **WIRELESS > Wireless**. The **Wireless** screen appears. In this example, the ZyXEL Device is using **WLAN Interface 1** in **Access Point** operating mode, and is currently set to use the **SSID04** profile.

**Figure 13** Tutorial: Wireless LAN: Before

| Wireless   | SSID | Security  | RADIUS | Layer-2 Isolation | MAC Filter |
|--|------|---|--------|-------------------|------------|
| WLAN Interface   |      | WLAN1   |        |                   |            |
| Operating Mode   |      | Access Point  |        |                   |            |
| 802.11 Mode  |      | 802.11b+g   |        |                   |            |
| <input checked="" type="checkbox"/> Super Mode                                       |      |   |        |                   |            |
| Choose Channel ID  |      | Channel-06 2437MHz or Scan  |        |                   |            |
| RTS/CTS Threshold  |      | 2346 (256 ~ 2346)   |        |                   |            |
| Fragmentation Threshold  |      | 2346 (256 ~ 2346) (Fragmentation threshold shall be an even number) |        |                   |            |
| Output Power   |      | 100%  |        |                   |            |
| SSID Profile   |      | SSID04  |        |                   |            |
| <input checked="" type="checkbox"/> Enable Spanning Tree Protocol (STP)              |      |   |        |                   |            |
| <input type="checkbox"/> Enable Roaming  |      |   |        |                   |            |
| (The STP and Roaming are common settings. The changes are for both WLAN Interfaces.) |      |   |        |                   |            |
| <div>Apply</div> <div>Reset</div>  |      |   |        |                   |            |

Select **MBSSID** from the **Operating Mode** drop-down list box. The screen displays as follows.

**Figure 14** Tutorial: Wireless LAN: Change Mode

| Wireless   | SSID                                | Security  | RADIUS | Layer-2 Isolation        | MAC Filter |
|--|-------------------------------------|---|--------|--------------------------|------------|
| WLAN Interface   |                                     | WLAN1   |        |                          |            |
| Operating Mode   |                                     | MBSSID  |        |                          |            |
| 802.11 Mode  |                                     | 802.11b+g   |        |                          |            |
| <input checked="" type="checkbox"/> Super Mode                                       |                                     |   |        |                          |            |
| Choose Channel ID  |                                     | Channel-06 2437MHz or Scan  |        |                          |            |
| RTS/CTS Threshold  |                                     | 2346 (256 ~ 2346)   |        |                          |            |
| Fragmentation Threshold  |                                     | 2346 (256 ~ 2346) (Fragmentation threshold shall be an even number) |        |                          |            |
| Output Power   |                                     | 100%  |        |                          |            |
| Select SSID Profile  |                                     |   |        |                          |            |
| Index  | Active                              | Profile   | Index  | Active                   | Profile    |
| 1  | <input type="checkbox"/>            | VoIP_SSID   | 5      | <input type="checkbox"/> | SSID03     |
| 2  | <input type="checkbox"/>            | Guest_SSID  | 6      | <input type="checkbox"/> | SSID03     |
| 3  | <input checked="" type="checkbox"/> | SSID04  | 7      | <input type="checkbox"/> | SSID03     |
| 4  | <input type="checkbox"/>            | SSID03  | 8      | <input type="checkbox"/> | SSID03     |
| <input checked="" type="checkbox"/> Enable Spanning Tree Protocol (STP)              |                                     |   |        |                          |            |
| <input type="checkbox"/> Enable Roaming  |                                     |   |        |                          |            |
| (The STP and Roaming are common settings. The changes are for both WLAN Interfaces.) |                                     |   |        |                          |            |
| <div>Apply</div> <div>Reset</div>  |                                     |   |        |                          |            |

This **Select SSID Profile** table allows you to activate or deactivate SSID profiles. Your wireless network was previously using the **SSID04** profile, so select **SSID04** in one of the **Profile** list boxes (number **3** in this example).

Select the **Active** box for the entry and click **Apply** to activate the profile. Your standard wireless network (**SSID04**) is now accessible to your wireless clients as before. You do not need to configure anything else for your standard network.

## 4.2.2 Configure the VoIP Network

Next, click **WIRELESS > SSID**. The following screen displays. Note that the **SSID04** SSID profile (the standard network) is using the **security01** security profile. You cannot change this security profile without changing the standard network's parameters, so when you set up security for the **VoIP\_SSID** and **Guest\_SSID** profiles you will need to set different security profiles.

**Figure 15** Tutorial: WIRELESS > SSID

| Wireless                         | SSID  | Security     | RADIUS  | Layer-2 Isolation | MAC Filter |      |                   |            |
|----------------------------------|-------|--------------|---------|-------------------|------------|------|-------------------|------------|
|                                  | Index | Profile Name | SSID    | Security          | RADIUS     | QoS  | Layer-2 Isolation | MAC Filter |
| <input checked="" type="radio"/> | 1     | VoIP_SSID    | ZyXEL01 | security01        | radius01   | VoIP | Disable           | Disable    |
| <input type="radio"/>            | 2     | Guest_SSID   | ZyXEL02 | security01        | radius01   | NONE | l2isolation01     | Disable    |
| <input type="radio"/>            | 3     | SSID03       | ZyXEL03 | security01        | radius01   | NONE | Disable           | Disable    |
| <input type="radio"/>            | 4     | SSID04       | ZyXEL04 | security01        | radius01   | NONE | Disable           | Disable    |
| <input type="radio"/>            | 5     | SSID05       | ZyXEL05 | security01        | radius01   | NONE | Disable           | Disable    |
| <input type="radio"/>            | 6     | SSID06       | ZyXEL06 | security01        | radius01   | NONE | Disable           | Disable    |
| <input type="radio"/>            | 7     | SSID07       | ZyXEL07 | security01        | radius01   | NONE | Disable           | Disable    |
| <input type="radio"/>            | 8     | SSID08       | ZyXEL08 | security08        | radius01   | NONE | Disable           | Disable    |
| <input type="radio"/>            | 9     | SSID09       | ZyXEL09 | security01        | radius01   | NONE | Disable           | Disable    |
| <input type="radio"/>            | 10    | SSID10       | ZyXEL10 | security01        | radius01   | NONE | Disable           | Disable    |
| <input type="radio"/>            | 11    | SSID11       | ZyXEL11 | security01        | radius01   | NONE | Disable           | Disable    |
| <input type="radio"/>            | 12    | SSID12       | ZyXEL12 | security01        | radius01   | NONE | Disable           | Disable    |
| <input type="radio"/>            | 13    | SSID13       | ZyXEL13 | security01        | radius01   | NONE | Disable           | Disable    |
| <input type="radio"/>            | 14    | SSID14       | ZyXEL14 | security01        | radius01   | NONE | Disable           | Disable    |
| <input type="radio"/>            | 15    | SSID15       | ZyXEL15 | security01        | radius01   | NONE | Disable           | Disable    |
| <input type="radio"/>            | 16    | SSID16       | ZyXEL16 | security01        | radius01   | NONE | Disable           | Disable    |

Edit

The Voice over IP (VoIP) network will use the pre-configured SSID profile, so select **VoIP\_SSID**'s radio button and click **Edit**. The following screen displays.

**Figure 16** Tutorial: VoIP SSID Profile Edit

| Wireless                            | SSID | Security          | RADIUS | Layer-2 Isolation | MAC Filter |
|-------------------------------------|------|-------------------|--------|-------------------|------------|
| <b>Name :</b>                       |      | <b>VoIP_SSID</b>  |        |                   |            |
| <b>SSID :</b>                       |      | VoIP_SSID_Example |        |                   |            |
| <b>Hide Name(SSID) :</b>            |      | Enable ▾          |        |                   |            |
| <b>Security :</b>                   |      | security02 ▾      |        |                   |            |
| <b>RADIUS :</b>                     |      | radius01 ▾        |        |                   |            |
| <b>QoS :</b>                        |      | <b>VoIP</b>       |        |                   |            |
| <b>L2 Isolation :</b>               |      | Disable ▾         |        |                   |            |
| <b>Intra-BSS Traffic blocking :</b> |      | Disable ▾         |        |                   |            |
| <b>MAC Filtering :</b>              |      | Disable ▾         |        |                   |            |
|                                     |      | Apply             |        | Reset             |            |

- Choose a new SSID for the VoIP network. In this example, enter **VOIP\_SSID\_Example**. Note that although the SSID changes, the SSID profile name (**VoIP\_SSID**) remains the same as before.
- Select **Enable** from the **Hide Name (SSID)** list box. You want only authorized company employees to use this network, so there is no need to broadcast the SSID to wireless clients scanning the area.
- The standard network (**SSID04**) is currently using the **security01** profile, so use a different profile for the VoIP network. If you used the **security01** profile, anyone who could access the standard network could access the VoIP wireless network. Select **security02** from the **Security** field.
- Leave all the other fields at their defaults and click **Apply**.

#### 4.2.2.1 Set Up Security for the VoIP Profile

Now you need to configure the security settings to use on the VoIP wireless network. Click the **Security** tab.

**Figure 17** Tutorial: VoIP Security

| Wireless                         | SSID  | Security     | RADIUS        | Layer-2 Isolation | MAC Filter |
|----------------------------------|-------|--------------|---------------|-------------------|------------|
| -                                | Index | Profile Name | Security Mode |                   |            |
| <input type="radio"/>            | 1     | security01   | WPA2.PSK      |                   |            |
| <input checked="" type="radio"/> | 2     | security02   | None          |                   |            |
| <input type="radio"/>            | 3     | security03   | None          |                   |            |
| <input type="radio"/>            | 4     | security04   | None          |                   |            |
| <input type="radio"/>            | 5     | security05   | None          |                   |            |
| <input type="radio"/>            | 6     | security06   | None          |                   |            |
| <input type="radio"/>            | 7     | security07   | None          |                   |            |
| <input type="radio"/>            | 8     | security08   | None          |                   |            |
| <input type="radio"/>            | 9     | security09   | None          |                   |            |
| <input type="radio"/>            | 10    | security10   | None          |                   |            |
| <input type="radio"/>            | 11    | security11   | None          |                   |            |
| <input type="radio"/>            | 12    | security12   | None          |                   |            |
| <input type="radio"/>            | 13    | security13   | None          |                   |            |
| <input type="radio"/>            | 14    | security14   | None          |                   |            |
| <input type="radio"/>            | 15    | security15   | None          |                   |            |
| <input type="radio"/>            | 16    | security16   | None          |                   |            |

You already chose to use the **security02** profile for this network, so select the radio button for **security02** and click **Edit**. The following screen appears.

**Figure 18** Tutorial: VoIP Security Profile Edit

| Wireless  | SSID | Security | RADIUS | Layer-2 Isolation | MAC Filter |
|---|------|----------|--------|-------------------|------------|
| <div> <div> Name : Security Mode : Pre-Shared Key : ReAuthentication Timer : Idle Timeout : Group Key Update Timer : </div> <div> <input type="text" value="VoIP_Security"/> <input type="text" value="WPA2-PSK"/> <input type="text" value="ThisismyWPA2-PSKpre-sharedkey"/> <input type="text" value="1800"/> ( in seconds) <input type="text" value="3600"/> ( in seconds) <input type="text" value="1800"/> ( in seconds) </div> </div> |      |          |        |                   |            |
| <div> <div>Apply</div> <div>Reset</div> </div>  |      |          |        |                   |            |

- Change the **Name** field to “VoIP\_Security” to make it easier to remember and identify.
- In this example, you do not have a RADIUS server for authentication, so select **WPA2-PSK** in the **Security Mode** field. WPA2-PSK provides strong security that anyone with a compatible wireless client can use, once they know the pre-shared key (PSK). Enter the PSK you want to use in your network in the **Pre-Shared Key** field. In this example, the PSK is “ThisismyWPA2-PSKpre-sharedkey”.

- Click **Apply**. The **WIRELESS > Security** screen displays. Ensure that the **Profile Name** for entry 2 displays “**VoIP\_Security**” and that the **Security Mode** is **WPA2-PSK**.

**Figure 19** Tutorial: VoIP Security: Updated

| Wireless | SSID | Security | RADIUS        | Layer-2 Isolation | MAC Filter |
|----------|------|----------|---------------|-------------------|------------|
|          |      |          |               |                   |            |
|          |      | Index    | Profile Name  | Security Mode     |            |
|          |      | 1        | security01    | None              |            |
|          |      | 2        | VoIP_Security | WPA2-PSK          |            |
|          |      | 3        | security03    | None              |            |
|          |      | 4        |               |                   |            |

#### 4.2.2.2 Activate the VoIP Profile

You need to activate the **VoIP\_SSID** profile before it can be used. Click the **Wireless** tab. In the **Select SSID Profile** table, select the **VoIP\_SSID** profile’s **Active** checkbox and click **Apply**.

**Figure 20** Tutorial: Activate VoIP Profile

Output Power 100%

Select SSID Profile

| Index | Active                              | Profile    | Index | Active                   | Profile |
|-------|-------------------------------------|------------|-------|--------------------------|---------|
| 1     | <input checked="" type="checkbox"/> | VoIP_SSID  | 5     | <input type="checkbox"/> | SSID03  |
| 2     | <input type="checkbox"/>            | Guest_SSID | 6     | <input type="checkbox"/> | SSID03  |
| 3     | <input checked="" type="checkbox"/> | SSID04     | 7     | <input type="checkbox"/> | SSID03  |
| 4     | <input type="checkbox"/>            | SSID03     | 8     | <input type="checkbox"/> | SSID03  |

☒ Enable Spanning Tree Protocol (STP)

Your VoIP wireless network is now ready to use. Any traffic using the **VoIP\_SSID** profile will be given the highest priority across the wireless network.

### 4.2.3 Configure the Guest Network

When you are setting up the wireless network for guests to your office, your primary concern is to keep your network secure while allowing access to certain resources (such as a network printer, or the Internet). For this reason, the pre-configured **Guest\_SSID** profile has layer-2 isolation and intra-BSS traffic blocking enabled by default. “Layer-2 isolation” means that a client accessing the network via the **Guest\_SSID** profile can access only certain pre-defined devices on the network (see [Section 9.1 on page 121](#)), and “intra-BSS traffic blocking” means that the client cannot access other clients on the same wireless network (see [Section 8.2 on page 117](#)).

Click **WIRELESS > SSID**. Select **Guest\_SSID**’s entry in the list and click **Edit**. The following screen appears.

**Figure 21** Tutorial: Guest Edit

| Wireless   | SSID | Security | RADIUS | Layer-2 Isolation | MAC Filter |
|--|------|----------|--------|-------------------|------------|
| <b>Profile Name :</b> Guest_SSID<br><b>SSID :</b> Guest_SSID_Example<br><b>Hide Name(SSID) :</b> Disable<br><b>Security :</b> security03<br><b>RADIUS :</b> radius01<br><b>QoS :</b> NONE<br><b>L2 Isolation :</b> l2isolation01<br><b>Intra-BSS Traffic blocking :</b> Enable<br><b>MAC Filtering :</b> Disable |      |          |        |                   |            |
| <div>Apply</div> <div>Reset</div>  |      |          |        |                   |            |

- Choose a new SSID for the guest network. In this example, enter **Guest\_SSID\_Example**. Note that although the SSID changes, the SSID profile name (**Guest\_SSID**) remains the same as before.
- Select **Disable** from the **Hide Name (SSID)** list box. This makes it easier for guests to configure their own computers' wireless clients to your network's settings.
- The standard network (SSID04) is already using the **security01** profile, and the VoIP network is using the **security02** profile (renamed **VoIP\_Security**) so select the **security03** profile from the **Security** field.
- Leave all the other fields at their defaults and click **Apply**.

#### 4.2.3.1 Set Up Security for the Guest Profile

Now you need to configure the security settings to use on the guest wireless network. Click the **Security** tab.

You already chose to use the **security03** profile for this network, so select **security03**'s entry in the list and click **Edit**. The following screen appears.

**Figure 22** Tutorial: Guest Security Profile Edit

| Wireless   | SSID | Security | RADIUS | Layer-2 Isolation | MAC Filter |
|--|------|----------|--------|-------------------|------------|
| <b>Name :</b> Guest_Security<br><b>Security Mode :</b> WPA-PSK<br><b>Pre-Shared Key :</b> ThisismyGuestWPAPre-shared-key<br><b>ReAuthentication Timer :</b> 1800 ( in seconds)<br><b>Idle Timeout :</b> 3600 ( in seconds)<br><b>Group Key Update Timer :</b> 1800 ( in seconds) |      |          |        |                   |            |
| <div>Apply</div> <div>Reset</div>  |      |          |        |                   |            |

- Change the **Name** field to "Guest\_Security" to make it easier to remember and identify.

- Select **WPA-PSK** in the **Security Mode** field. WPA-PSK provides strong security that is supported by most wireless clients. Even though your **Guest\_SSID** clients do not have access to sensitive information on the network, you should not leave the network without security. An attacker could still cause damage to the network or intercept unsecured communications.
- Enter the PSK you want to use in your network in the **Pre-Shared Key** field. In this example, the PSK is “ThisismyGuestWPApre-sharedkey”.
- Click **Apply**. The **WIRELESS > Security** screen displays. Ensure that the **Profile Name** for entry 3 displays “**Guest\_Security**” and that the **Security Mode** is **WPA-PSK**.

**Figure 23** Tutorial: Guest Security: Updated

| Wireless | SSID  | Security       | RADIUS        | Layer-2 Isolation | MAC Filter |
|----------|-------|----------------|---------------|-------------------|------------|
|          |       |                |               |                   |            |
|          | Index | Profile Name   | Security Mode |                   |            |
|          | 1     | security01     | WPA2-PSK      |                   |            |
|          | 2     | VoIP_Security  | WPA2-PSK      |                   |            |
|          | 3     | Guest_Security | WPA-PSK       |                   |            |
|          | 4     | security04     | None          |                   |            |

#### 4.2.3.2 Set up Layer 2 Isolation

Configure layer 2 isolation to control the specific devices you want the users on your guest network to access. Click **WIRELESS > Layer-2 Isolation**. The following screen appears.

**Figure 24** Tutorial: Layer 2 Isolation

| Wireless | SSID  | Security      | RADIUS | Layer-2 Isolation | MAC Filter |
|----------|-------|---------------|--------|-------------------|------------|
|          |       |               |        |                   |            |
|          | Index | Profile Name  |        |                   |            |
|          | 1     | I2isolation01 |        |                   |            |
|          | 2     | I2isolation02 |        |                   |            |
|          | 3     | I2isolation03 |        |                   |            |
|          | 4     | I2isolation04 |        |                   |            |
|          | 5     | I2isolation05 |        |                   |            |
|          | 14    | I2isolation14 |        |                   |            |
|          | 15    | I2isolation15 |        |                   |            |
|          | 16    | I2isolation16 |        |                   |            |

[Edit](#)

The **Guest\_SSID** network uses the **I2isolation01** profile by default, so select its entry and click **Edit**. The following screen displays.

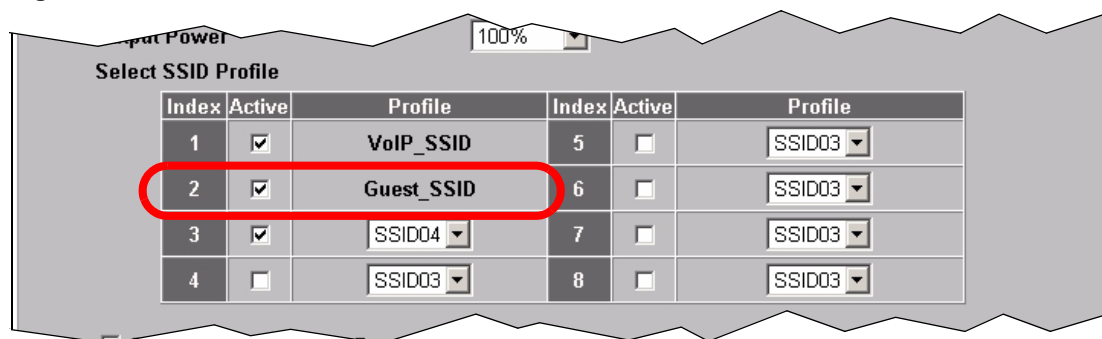
**Figure 25** Tutorial: Layer 2 Isolation Profile

| Wireless                               | SSID              | Security        | RADIUS | Layer-2 Isolation | MAC Filter  |
|--|-------------------|-----------------|--------|-------------------|-------------|
| <b>Layer-2 Isolation Configuration</b> |                   |                 |        |                   |             |
| Profile Name                           |                   | l2isolation01   |        |                   |             |
| Allow devices with these MAC addresses |                   |                 |        |                   |             |
| Index                                  | MAC Address       | Description     | Index  | MAC Address       | Description |
| 1                                      | 00:AA:00:AA:00:AA | network router  | 17     | 00:00:00:00:00:00 |             |
| 2                                      | AA:00:AA:00:AA:00 | network printer | 18     | 00:00:00:00:00:00 |             |
| 3                                      | 00:00:00:00:00:00 |                 | 19     | 00:00:00:00:00:00 |             |
| 4                                      | 00:00:00:00:00:00 |                 | 20     | 00:00:00:00:00:00 |             |
| 5                                      | 00:00:00:00:00:00 |                 | 21     | 00:00:00:00:00:00 |             |
| 6                                      | 00:00:00:00:00:00 |                 | 22     | 00:00:00:00:00:00 |             |
| 7                                      | 00:00:00:00:00:00 |                 | 23     | 00:00:00:00:00:00 |             |
| 8                                      | 00:00:00:00:00:00 |                 | 24     | 00:00:00:00:00:00 |             |
| 9                                      | 00:00:00:00:00:00 |                 | 25     | 00:00:00:00:00:00 |             |
| 10                                     | 00:00:00:00:00:00 |                 | 26     | 00:00:00:00:00:00 |             |
| 11                                     | 00:00:00:00:00:00 |                 | 27     | 00:00:00:00:00:00 |             |
| 12                                     | 00:00:00:00:00:00 |                 | 28     | 00:00:00:00:00:00 |             |
| 13                                     | 00:00:00:00:00:00 |                 | 29     | 00:00:00:00:00:00 |             |
| 14                                     | 00:00:00:00:00:00 |                 | 30     | 00:00:00:00:00:00 |             |
| 15                                     | 00:00:00:00:00:00 |                 | 31     | 00:00:00:00:00:00 |             |
| 16                                     | 00:00:00:00:00:00 |                 | 32     | 00:00:00:00:00:00 |             |

Enter the MAC addresses and descriptions of the two network devices you want users on the guest network to be able to access: the main network router (00:AA:00:AA:00:AA) and the network printer (AA:00:AA:00:AA:00). Click **Apply**.

#### 4.2.3.3 Activate the Guest Profile

You need to activate the **Guest\_SSID** profile before it can be used. Click the **Wireless** tab. In the **Select SSID Profile** table, select the check box for the **Guest\_SSID** profile and click **Apply**.

**Figure 26** Tutorial: Activate Guest Profile

Your guest wireless network is now ready to use.

#### 4.2.4 Testing the Wireless Networks

To make sure that the three networks are correctly configured, do the following.

- On a computer with a wireless client, scan for access points. You should see the **Guest\_SSID** network, but not the **VoIP\_SSID** network. If you can see the **VoIP\_SSID** network, go to its **SSID Edit** screen and make sure **Hide Name (SSID)** is set to **Enable**. Whether or not you see the standard network's SSID (**SSID04**) depends on whether "hide SSID" is enabled.
- Try to access each network using the correct security settings, and then using incorrect security settings, such as the WPA-PSK for another active network. If the behavior is different from expected (for example, if you can access the VoIP wireless network using the security settings for the **Guest\_SSID** wireless network) check that the SSID profile is set to use the correct security profile, and that the settings of the security profile are correct.
- Access the **Guest\_SSID** network and try to access other resources than those specified in the Layer 2 Isolation (**l2isolation01**) profile screen.

You can use the ping utility to do this. Click **Start > Run...** and enter "cmd" in the **Open:** field. Click **OK**. At the **c:\>** prompt, enter "ping 192.168.1.10" (substitute the IP address of a real device on your network that is not on the layer 2 isolation list). If you receive a reply, check the settings in the **WIRELESS > Layer-2 Isolation > Edit** screen, and ensure that the correct layer 2 isolation profile is enabled in the **Guest\_SSID** profile screen.

### 4.3 How to Set Up and Use Rogue AP Detection

This example shows you how to configure the rogue AP detection feature on the ZyXEL Device.

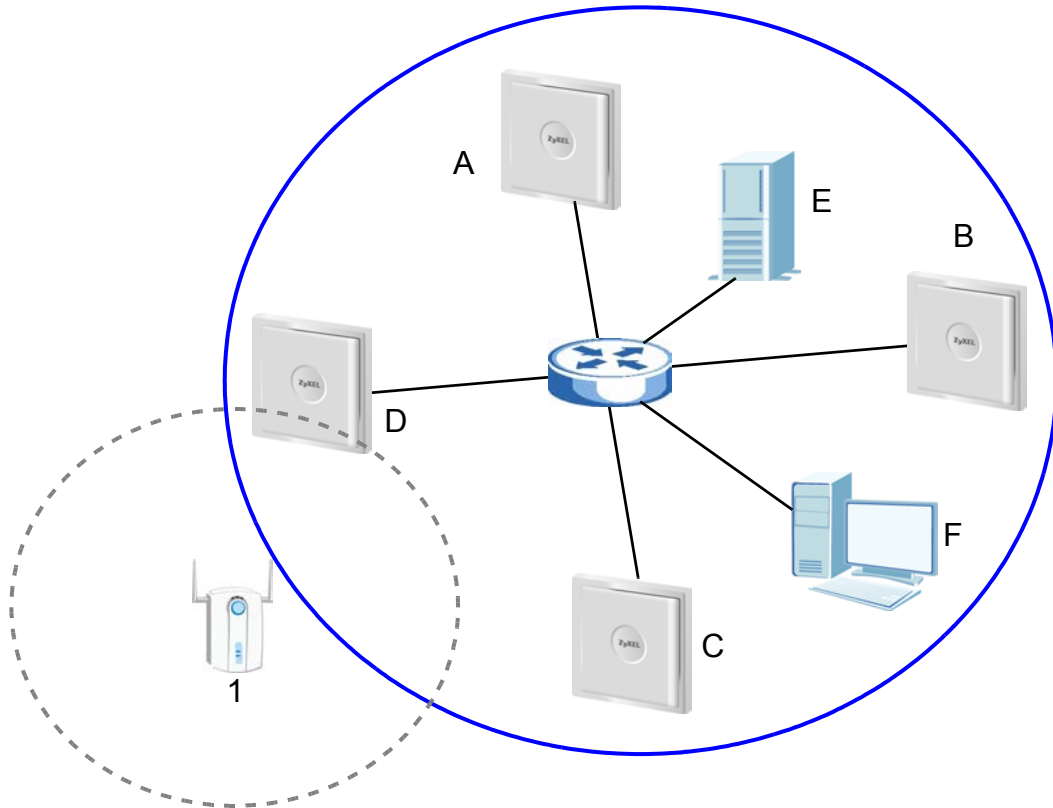
A rogue AP is a wireless access point operating in a network's coverage area that is not a sanctioned part of that network. The example also shows how to set the ZyXEL Device to send out e-mail alerts whenever it detects a rogue wireless access point. See [Chapter 11 on page 137](#) for background information on the rogue AP function and security considerations.

In this example, you want to ensure that your company's data is not accessible to an attacker gaining entry to your wireless network through a rogue AP.

Your wireless network operates in an office building. It consists of four access points (all ZyXEL Devices) and a variable number of wireless clients. You also know that the coffee shop on the ground floor has a wireless network consisting of a single access point, which can be detected and accessed from your floor of the building. There are no other static wireless networks in your coverage area.

The following diagram shows the wireless networks in your area. Your access points are marked **A**, **B**, **C** and **D**. You also have a network mail/file server, marked **E**, and a computer, marked **F**, connected to the wired network. The coffee shop's access point is marked **1**.

**Figure 27** Tutorial: Wireless Network Example



In the figure, the solid circle represents the range of your wireless network, and the dashed circle represents the extent of the coffee shop's wireless network. Note that the two networks overlap. This means that one or more of your APs can detect the AP (**1**) in the other wireless network.

When configuring the rogue AP feature on your ZyXEL Devices in this example, you will need to use the information in the following table. You need the IP addresses of your APs to access their Web configurators, and you need the MAC address of each AP to configure the friendly AP list. You need the IP address of the mail server to set up e-mail alerts.

**Table 3** Tutorial: Rogue AP Example Information

| DEVICE                | IP ADDRESS  | MAC ADDRESS       |
|-----------------------|-------------|-------------------|
| Access Point <b>A</b> | 192.168.1.1 | 00:AA:00:AA:00:AA |
| Access Point <b>B</b> | 192.168.1.2 | AA:00:AA:00:AA:00 |
| Access Point <b>C</b> | 192.168.1.3 | A0:0A:A0:0A:A0:0A |

**Table 3** Tutorial: Rogue AP Example Information

| DEVICE                      | IP ADDRESS   | MAC ADDRESS       |
|-----------------------------|--------------|-------------------|
| Access Point <b>D</b>       | 192.168.1.4  | 0A:A0:0A:A0:0A:A0 |
| File / Mail Server <b>E</b> | 192.168.1.25 | N/A               |
| Access Point <b>1</b>       | UNKNOWN      | AF:AF:AF:FA:FA:FA |



The ZyXEL Device can detect the MAC addresses of APs automatically. However, it is more secure to obtain the correct MAC addresses from another source and add them to the friendly AP list manually. For example, an attacker's AP mimicking the correct SSID could be placed on the friendly AP list by accident, if selected from the list of auto-detected APs. In this example you have spoken to the coffee shop's owner, who has told you the correct MAC address of his AP.

In this example, you will do the following things.

- 1 Set up and save a friendly AP list.
- 2 Activate periodic Rogue AP Detection.
- 3 Set up e-mail alerts.
- 4 Configure your other access points.
- 5 Test the setup.

### 4.3.1 Set Up and Save a Friendly AP list

Take the following steps to set up and save a list of access points you want to allow in your network's coverage area.

- 1 On a computer connected to the wired network (**F** in the previous figure), open your Internet browser and enter the URL of access point **A** (192.168.1.1). Login to the Web configurator and click **ROGUE AP > Friendly AP**. The following screen displays.

**Figure 28** Tutorial: Friendly AP (Before Data Entry)

| Configuration        |             |                      |         |                                    |             |
|----------------------|-------------|----------------------|---------|------------------------------------|-------------|
| Friendly AP          |             |                      |         |                                    |             |
| Rogue AP             |             |                      |         |                                    |             |
| Add Friendly AP      |             |                      |         |                                    |             |
| MAC Address          |             | Description          |         |                                    |             |
| <input type="text"/> |             | <input type="text"/> |         | <input type="button" value="Add"/> |             |
| Friendly AP List     |             |                      |         |                                    |             |
| #                    | MAC Address | SSID                 | Channel | Security                           | Description |
| <br>                 |             |                      |         |                                    |             |

- 2 Fill in the **MAC Address** and **Description** fields as in the following table. Click **Add** after you enter the details of each AP to include it in the list.

**Table 4** Tutorial: Friendly AP Information

| MAC ADDRESS       | DESCRIPTION                  |
|-------------------|------------------------------|
| 00:AA:00:AA:00:AA | My Access Point _A_          |
| AA:00:AA:00:AA:00 | My Access Point _B_          |
| A0:0A:A0:0A:A0:0A | My Access Point _C_          |
| 0A:A0:0A:A0:0A:A0 | My Access Point _D_          |
| AF:AF:AF:FA:FA:FA | Coffee Shop Access Point _1_ |



You can add APs that are not part of your network to the friendly AP list, as long as you know that they do not pose a threat to your network's security.

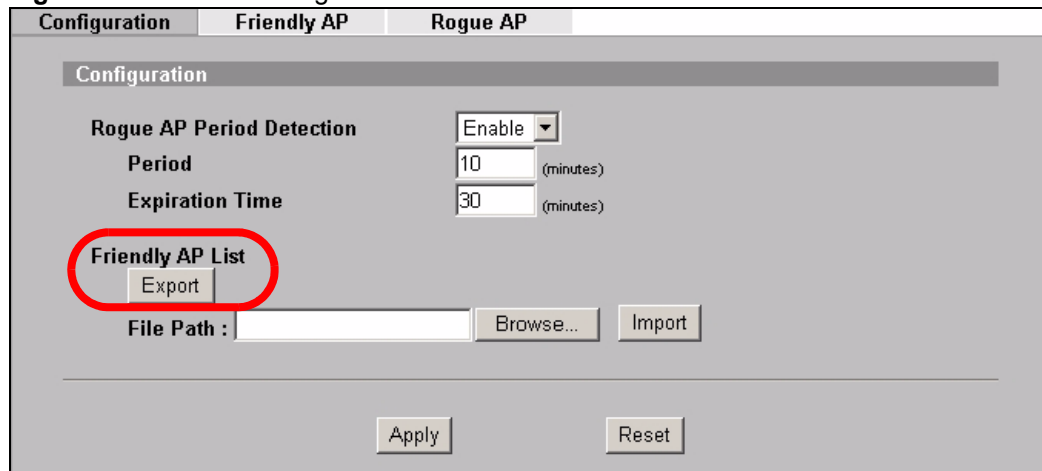
The **Friendly AP** screen now appears as follows.

**Figure 29** Tutorial: Friendly AP (After Data Entry)

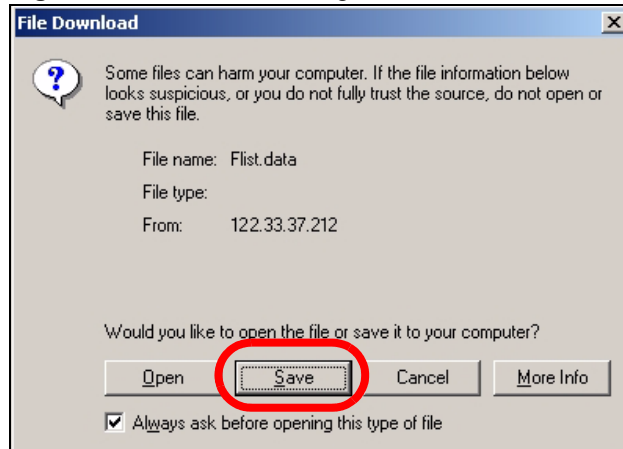
| Configuration   Friendly AP   Rogue AP |                   |                      |         |          |           |                                    |  |
|--|-------------------|----------------------|---------|----------|-----------|------------------------------------|--|
| Add Friendly AP                        |                   |                      |         |          |           |                                    |  |
| MAC Address                            |                   | Description          |         |          |           |                                    |  |
| <input type="text"/>                   |                   | <input type="text"/> |         |          |           | <input type="button" value="Add"/> |  |
| Friendly AP List                       |                   |                      |         |          |           |                                    |  |
| #                                      | MAC Address       | SSID                 | Channel | Security | Last Seen | Description                        |  |
| 1                                      | 00:aa:00:aa:00:aa | N/A                  | N/A     | N/A      | 4:00:02   | My Access Point _A_                |  |
| 2                                      | aa:00:aa:00:aa:00 | N/A                  | N/A     | N/A      | 4:00:02   | My Access Point _B_                |  |
| 3                                      | a0:0a:a0:0a:a0:0a | N/A                  | N/A     | N/A      | 4:00:02   | My Access Point _C_                |  |
| 4                                      | 0a:a0:0a:a0:0a:a0 | N/A                  | N/A     | N/A      | 4:00:00   | My Access Point _D_                |  |
| 5                                      | af:af:af:fa:fa:fa | N/A                  | N/A     | N/A      | 3:50:00   | Coffee Shop Access Point _1_       |  |

- 3 Next, you will save the list of friendly APs in order to provide a backup and upload it to your other access points.

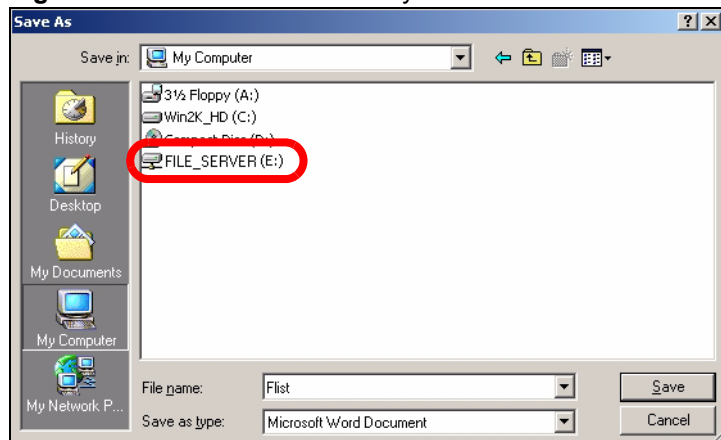
Click the **Configuration** tab. The following screen appears.

**Figure 30** Tutorial: Configuration

- 4 Click **Export**. If a window similar to the following appears, click **Save**.

**Figure 31** Tutorial: Warning

- 5 Save the friendly AP list somewhere it can be accessed by all the other access points on the network. In this example, save it on the network file server (E in [Figure 27 on page 63](#)). The default filename is "Flist".

**Figure 32** Tutorial: Save Friendly AP list

### 4.3.2 Activate Periodic Rogue AP Detection

Take the following steps to activate rogue AP detection on the first of your ZyXEL Devices.

- 1 In the **ROGUE AP > Configuration** screen, select **Enable** from the **Rogue AP Period Detection** field.

**Figure 33** Tutorial: Periodic Rogue AP Detection

The screenshot shows the ZyXEL web interface for configuring Rogue AP detection. The 'Rogue AP' tab is active. In the 'Configuration' section, the 'Rogue AP Period Detection' dropdown is set to 'Enable'. Below it, the 'Period' is set to '10' minutes and the 'Expiration Time' is set to '30' minutes. The 'Friendly AP List' section includes an 'Export' button, a 'File Path' input field, a 'Browse...' button, and an 'Import' button. At the bottom of the page are 'Apply' and 'Reset' buttons.

- 2 In the **Period** field, enter how often you want the ZyXEL Device to scan for rogue APs. You can have the ZyXEL Device scan anywhere from once every ten minutes to once every hour. In this example, enter “10”.
- 3 In the **Expiration Time** field, enter how long an AP’s entry can remain in the list before the ZyXEL Device discards it from the list when the AP is no longer active. In this example, enter “30”.
- 4 Click **Apply**.

### 4.3.3 Set Up E-mail Logs

In this section, you will configure the first of your four APs to send a log message to your e-mail inbox whenever a rogue AP is discovered in your wireless network’s coverage area.

- 1 Click **LOGS > Log Settings**. The following screen appears.

**Figure 34** Tutorial: Log Settings

**View Log** **Log Settings**

**Address Info:**

**Mail Server:** 192.168.1.25 (Outgoing SMTP Server NAME or IP Address)

**Mail Subject:** ALERT\_Access\_Point\_A

**Send log to:** (E-Mail Address)

**Send alerts to:** myname@myfirm.com (E-Mail Address)

☐ SMTP Authentication

**User NAME:**

**Password:**

**Syslog Logging:**

☐ Active

**Syslog IP Address:** 0.0.0.0 (Server NAME or IP Address)

**Log Facility:** Local 1

**Send Log:**

**Log Schedule:** None

**Day for Sending Log:** Sunday

**Time for Sending Log:** 0 (hour) 0 (minute)

☐ Clear log after sending mail

**Log**

☐ System Maintenance

☐ System Errors

☐ PKI

☐ SSL/TLS

☐ 802.1x

☐ Wireless

☐ Internal RADIUS Server

☐ Rogue AP Detection

**Send immediate alert**

☒ System Errors

☐ PKI

☒ Rogue AP Detection

**Apply** **Reset**

- In this example, your mail server's IP address is **192.168.1.25**. Enter this IP address in the **Mail Server** field.
- Enter a subject line for the alert e-mails in the **Mail Subject** field. Choose a subject that is eye-catching and identifies the access point - in this example, "ALERT\_Access\_Point\_A".
- Enter the email address to which you want alerts to be sent (**myname@myfirm.com**, in this example).
- In the **Send Immediate Alert** section, select the events you want to trigger immediate e-mails. Ensure that **Rogue AP Detection** is selected.
- Click **Apply**.

#### 4.3.4 Configure Your Other Access Points

Access point A is now configured to do the following.

- Scan for access points in its coverage area every ten minutes.
- Recognize friendly access points from a list.
- Send immediate alerts to your email account if it detects an access point not on the list.

Now you need to configure the other wireless access points on your network to do the same things.

For each access point, take the following steps.

- 1 From a computer on the wired network, enter the access point's IP address and login to its Web configurator. See [Table 3 on page 63](#) for the example IP addresses.
- 2 Import the friendly AP list. Click **ROGUE AP > Configuration > Browse...** Find the "Flist" file where you previously saved it on the network and click **Open**.
- 3 Click **Import**. Check the **ROGUE AP > Friendly AP** screen to ensure that the friendly AP list has been correctly uploaded.
- 4 Activate periodic rogue AP detection. See [Section 4.3.2 on page 67](#).
- 5 Set up e-mail logs as in [Section 4.3.3 on page 67](#), but change the **Mail Subject** field so you can tell which AP the alerts come from ("ALERT\_Access\_Point\_B", etc.)

### 4.3.5 Test the Setup

Next, test your setup to ensure it is correctly configured.

- Log into each AP's Web configurator and click **ROGUE AP > Rogue AP**. Click **Refresh**. If any of the MAC addresses from [Table 4 on page 65](#) appear in the list, the friendly AP function may be incorrectly configured - check the **ROGUE AP > Friendly AP** screen. If any entries appear in the rogue AP list that are not in [Table 4 on page 65](#), write down the AP's MAC address for future reference and check your e-mail inbox. If you have received a rogue AP alert, email alerts are correctly configured on that ZyXEL Device.
- If you have another access point that is not used in your network, make a note of its MAC address and set it up next to each of your ZyXEL Devices in turn while the network is running.

Either wait for at least ten minutes (to ensure the ZyXEL Device performs a scan in that time) or login to the ZyXEL Device's Web configurator and click **ROGUE AP > Rogue AP > Refresh** to have the ZyXEL Device perform a scan immediately.

- Check the **ROGUE AP > Rogue AP** screen. You should see an entry in the list with the same MAC address as your "rogue" AP.
- Check the **LOGS > View Logs** screen. You should see a **Rogue AP Detection** entry in red text, including the MAC address of your "rogue" AP.
- Check your e-mail. You should have received at least one e-mail alert (your other ZyXEL Devices may also have sent alerts, depending on their proximity and the output power of your "rogue" AP).

## 4.4 Using Multiple MAC Filters and L-2 Isolation Profiles

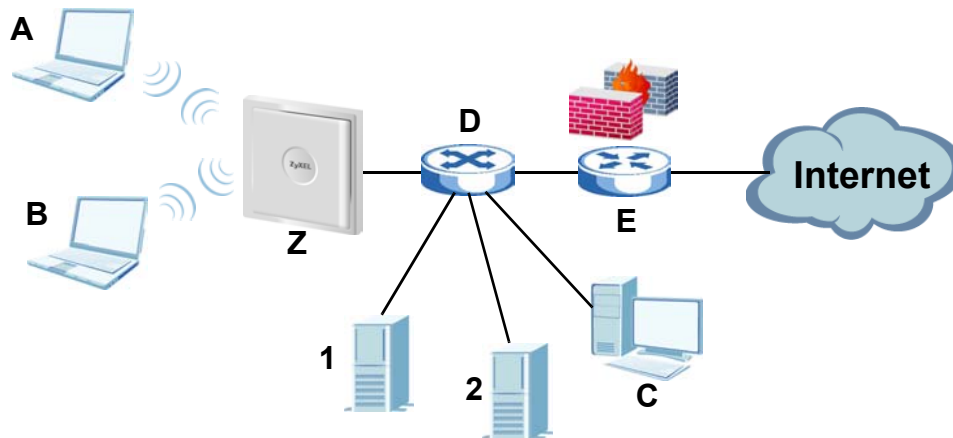
This example shows you how to allow certain users to access only specific parts of your network. You can do this by using multiple MAC filters and layer-2 isolation profiles.

### 4.4.1 Scenario

In this example, you run a company network in which certain employees must wirelessly access secure file servers containing valuable proprietary data.

You have two secure servers (**1** and **2** in the following figure). Wireless user “Alice” (**A**) needs to access server **1** (but should not access server **2**) and wireless user “Bob” (**B**) needs to access server **2** (but should not access server **1**). Your ZyXEL Device is marked **Z**. **C** is a workstation on your wired network, **D** is your main network switch, and **E** is the security gateway you use to connect to the Internet.

**Figure 35** Tutorial: Example Network



## 4.4.2 Your Requirements

- 1 You want to set up a wireless network to allow only Alice to access Server **1** and the Internet.
- 2 You want to set up a second wireless network to allow only Bob to access Server **2** and the Internet.

## 4.4.3 Setup

In this example, you have already set up the ZyXEL Device in MBSSID mode (see [Chapter 8 on page 113](#)). It uses two SSID profiles simultaneously. You have configured each SSID profile as shown in the following table.

**Table 5** Tutorial: SSID Profile Security Settings

| SSID Profile Name          | SERVER_1  | SERVER_2  |
|----------------------------|---|---|
| SSID                       | SSID_S1   | SSID_S2   |
| Security                   | Security Profile <b>security03</b> :<br>WPA2-PSK<br>Hide SSID | Security Profile <b>security04</b> :<br>WPA2-PSK<br>Hide SSID |
| Intra-BSS traffic blocking | Enabled   | Enabled   |

Each SSID profile already uses a different pre-shared key.

In this example, you will configure access limitations for each SSID profile. To do this, you will take the following steps.

- 1 Configure the **SERVER\_1** network’s SSID profile to use specific MAC filter and layer-2 isolation profiles.

- 2 Configure the **SERVER\_1** network's MAC filter profile.
- 3 Configure the **SERVER\_1** network's layer-2 isolation profile.
- 4 Repeat steps 1 ~ 3 for the **SERVER\_2** network.
- 5 Check your settings and test the configuration.

To configure layer-2 isolation, you need to know the MAC addresses of the devices on your network, which are as follows.

**Table 6** Tutorial: Example Network MAC Addresses

| DEVICE           | LABEL | MAC ADDRESS       |
|------------------|-------|-------------------|
| ZyXEL Device     | Z     | BB:AA:99:88:77:66 |
| Secure Server 1  | 1     | AA:99:88:77:66:55 |
| Secure Server 2  | 2     | 99:88:77:66:55:44 |
| Workstation      | C     | 88:77:66:55:44:33 |
| Switch           | D     | 77:66:55:44:33:22 |
| Security gateway | E     | 66:55:44:33:22:11 |

To configure MAC filtering, you need to know the MAC addresses of the devices Alice and Bob use to connect to the network, which are as follows.

**Table 7** Tutorial: Example User MAC Addresses

| USER  | MAC ADDRESS       |
|-------|-------------------|
| Alice | 11:22:33:44:55:66 |
| Bob   | 22:33:44:55:66:77 |

#### 4.4.4 Configure the **SERVER\_1** Network

First, you will set up the **SERVER\_1** network which allows Alice to access secure server **1** via the network switch.

You will configure the MAC filter to restrict access to Alice alone, and then configure layer-2 isolation to allow her to access only the network switch, the file server and the Internet security gateway.

Take the following steps to configure the **SERVER\_1** network.

- 1 Log into the ZyXEL Device's Web Configurator and click **WIRELESS > SSID**. The following screen displays, showing the SSID profiles you already configured.

**Figure 36** Tutorial: SSID Profile

| Wireless | SSID         | Security | RADIUS     | Layer-2 Isolation | MAC Filter |                   |            |
|----------|--------------|----------|------------|-------------------|------------|-------------------|------------|
| SERVER_1 |              |          |            |                   |            |                   |            |
| Index    | Profile Name | SSID     | Security   | RADIUS            | QoS        | Layer-2 Isolation | MAC Filter |
| 1        | VoIP_SSID    | ZyXEL01  | security01 | radius01          | VoIP       | Disable           | Disable    |
| 2        | Guest_SSID   | ZyXEL02  | security01 | radius01          | NONE       | I2isolation01     | Disable    |
| 3        | SERVER_1     | SSID03   | security03 | radius01          | NONE       | Disable           | Disable    |
| 4        | SERVER_2     | SSID04   | security04 | radius01          | NONE       | Disable           | Disable    |
| 5        | SSID05       | ZyXEL05  | security03 | radius01          | NONE       | Disable           | Disable    |
| 6        | SSID06       | ZyXEL06  | security01 | radius01          | NONE       | Disable           | Disable    |
| 7        | SSID07       | ZyXEL07  | security01 | radius01          | NONE       | Disable           | Disable    |
| 8        | SSID08       | ZyXEL08  | security01 | radius01          | NONE       | Disable           | Disable    |
| 9        | SSID09       | ZyXEL09  | security01 | radius01          | NONE       | Disable           | Disable    |
| 10       | SSID10       | ZyXEL10  | security01 | radius01          | NONE       | Disable           | Disable    |
| 11       | SSID11       | ZyXEL11  | security01 | radius01          | NONE       | Disable           | Disable    |
| 12       | SSID12       | ZyXEL12  | security01 | radius01          | NONE       | Disable           | Disable    |
| 13       | SSID13       | ZyXEL13  | security01 | radius01          | NONE       | Disable           | Disable    |
| 14       | SSID14       | ZyXEL14  | security01 | radius01          | NONE       | Disable           | Disable    |
| 15       | SSID15       | ZyXEL15  | security01 | radius01          | NONE       | Disable           | Disable    |
| 16       | SSID16       | ZyXEL16  | security01 | radius01          | NONE       | Disable           | Disable    |

- 2 Select **SERVER\_1**'s entry and click **Edit**. The following screen displays.

**Figure 37** Tutorial: SSID Edit

| Wireless  | SSID | Security | RADIUS | Layer-2 Isolation | MAC Filter |
|---|------|----------|--------|-------------------|------------|
| Profile Name : <input type="text" value="SERVER_1"/><br>SSID : <input type="text" value="SSID03"/><br>Hide Name(SSID) : <input type="text" value="Enable"/><br>Security : <input type="text" value="security03"/><br>RADIUS : <input type="text" value="radius01"/><br>QoS : <input type="text" value="NONE"/><br>L2 Isolation : <input type="text" value="I2isolation03"/><br>Intra-BSS Traffic blocking : <input type="text" value="Enable"/><br>MAC Filtering : <input type="text" value="macfilter03"/><br><div style="text-align: center;"> <input type="button" value="Apply"/> <input type="button" value="Reset"/> </div> |      |          |        |                   |            |

Select **I2Isolation03** in the **L2 Isolation** field, and select **macfilter03** in the **MAC Filtering** field. Click **Apply**.

- 3 Click the **Layer-2 Isolation** tab. When the **Layer-2 Isolation** screen appears, select **L2Isolation03**'s entry and click **Edit**. The following screen displays.

**Figure 38** Tutorial: Layer-2 Isolation Edit

| Wireless                               | SSID              | Security         | RADIUS | Layer-2 Isolation | MAC Filter  |
|--|-------------------|------------------|--------|-------------------|-------------|
| <b>Layer-2 Isolation Configuration</b> |                   |                  |        |                   |             |
| Profile Name                           |                   | L-2-ISO_SERVER_1 |        |                   |             |
| Allow devices with these MAC addresses |                   |                  |        |                   |             |
| Index                                  | MAC Address       | Description      | Index  | MAC Address       | Description |
| 1                                      | 77:66:55:44:33:22 | NET_SWITCH       | 17     | 00:00:00:00:00:00 |             |
| 2                                      | AA:99:88:77:66:55 | SERVER_1         | 18     | 00:00:00:00:00:00 |             |
| 3                                      | 66:55:44:33:22:11 | GATEWAY          | 19     | 00:00:00:00:00:00 |             |
| 4                                      | 00:00:00:00:00:00 |                  | 20     | 00:00:00:00:00:00 |             |

Enter the network switch's **MAC Address** and add a **Description** ("NET\_SWITCH" in this case) in **Set 1**'s entry.

Enter server 1's **MAC Address** and add a **Description** ("SERVER\_1" in this case) in **Set 2**'s entry.

Change the **Profile Name** to "L-2-ISO\_SERVER\_1" and click **Apply**. You have restricted users on the **SERVER\_1** network to access only the devices with the MAC addresses you entered.

- Click the **MAC Filter** tab. When the **MAC Filter** screen appears, select **macfilter03**'s entry and click **Edit**.

Enter the MAC address of the device Alice uses to connect to the network in **Index 1**'s **MAC Address** field and enter her name in the **Description** field, as shown in the following figure. Change the **Profile Name** to "MacFilter\_SERVER\_1". Select **Allow Association** from the **Filter Action** field and click **Apply**.

**Figure 39** Tutorial: MAC Filter Edit (SERVER\_1)

| Wireless                  | SSID              | Security           | RADIUS | Layer-2 Isolation | MAC Filter  |
|---------------------------|-------------------|--------------------|--------|-------------------|-------------|
| <b>MAC Address Filter</b> |                   |                    |        |                   |             |
| Profile Name              |                   | MacFilter_SERVER_1 |        |                   |             |
| Filter Action             |                   | Allow Association  |        |                   |             |
| Index                     | MAC Address       | Description        | Index  | MAC Address       | Description |
| 1                         | 11:22:33:44:55:66 | Alice              | 17     | 00:00:00:00:00:00 |             |
| 2                         | 00:00:00:00:00:00 |                    | 18     | 00:00:00:00:00:00 |             |
| 3                         |                   |                    |        |                   |             |

You have restricted access to the **SERVER\_1** network to only the networking device whose MAC address you entered. The **SERVER\_1** network is now configured.

#### 4.4.5 Configure the SERVER\_2 Network

Next, you will configure the **SERVER\_2** network that allows Bob to access secure server 2 and the Internet.

To do this, repeat the procedure in [Section 4.4.4 on page 71](#), substituting the following information.

**Table 8** Tutorial: SERVER\_2 Network Information

|   |   |
|---|---|
| <b>SSID Screen</b>                              |   |
| Index   | 4   |
| Profile Name                                    | SERVER_2  |
| <b>SSID Edit (SERVER_2) Screen</b>              |   |
| L2 Isolation                                    | L2Isolation04   |
| MAC Filtering                                   | macfilter04   |
| <b>Layer-2 Isolation (L2Isolation04) Screen</b> |   |
| Profile Name                                    | L-2-ISO_SERVER-2  |
| Set 1   | MAC Address: 77:66:55:44:33:22<br>Description: NET_SWITCH |
| Set 2   | MAC Address: 99:88:77:66:55:44<br>Description: SERVER_2   |
| Set 3   | MAC Address: 66:55:44:33:22:11<br>Description: GATEWAY    |
| <b>MAC Filter (macfilter04) Edit Screen</b>     |   |
| Profile Name                                    | MacFilter_SERVER_2  |
| Set 1   | MAC Address: 22:33:44:55:66:77<br>Description: Bob        |

## 4.4.6 Checking your Settings and Testing the Configuration

Use the following sections to ensure that your wireless networks are set up correctly.

### 4.4.6.1 Checking Settings

Take the following steps to check that the ZyXEL Device is using the correct SSIDs, MAC filters and layer-2 isolation profiles.

- 1 Click **WIRELESS > Wireless**. Check that the **Operating Mode** is **MBSSID** and that the correct SSID profiles are selected and activated, as shown in the following figure.

**Figure 40** Tutorial: SSID Profiles Activated

| Wireless  | SSID                                | Security              | RADIUS | Layer-2 Isolation        | MAC Filter            |       |        |         |       |        |         |   |                          |           |   |                          |                       |   |                          |            |   |                          |                       |   |                                     |                       |   |                          |                       |   |                                     |                       |   |                          |                       |
|---|-------------------------------------|-----------------------|--------|--------------------------|-----------------------|-------|--------|---------|-------|--------|---------|---|--------------------------|-----------|---|--------------------------|-----------------------|---|--------------------------|------------|---|--------------------------|-----------------------|---|-------------------------------------|-----------------------|---|--------------------------|-----------------------|---|-------------------------------------|-----------------------|---|--------------------------|-----------------------|
| <b>WLAN Interface</b> <span>WLAN1</span><br><b>Operating Mode</b> <span>MBSSID</span><br><b>802.11 Mode</b> <span>802.11b+g</span><br><input checked="" type="checkbox"/> <b>Super Mode</b><br><b>Choose Channel ID</b> <span>Channel-06 2437MHz</span> or <span>Scan</span><br><b>RTS/CTS Threshold</b> <span>2346</span> (256 ~ 2346)<br><b>Fragmentation Threshold</b> <span>2346</span> (256 ~ 2346) (Fragmentation threshold shall be an even number)<br><b>Output Power</b> <span>100%</span><br><b>Select SSID Profile</b> <table border="1"> <thead> <tr> <th>Index</th> <th>Active</th> <th>Profile</th> <th>Index</th> <th>Active</th> <th>Profile</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="checkbox"/></td> <td>VoIP_SSID</td> <td>5</td> <td><input type="checkbox"/></td> <td><span>SERVER_1</span></td> </tr> <tr> <td>2</td> <td><input type="checkbox"/></td> <td>Guest_SSID</td> <td>6</td> <td><input type="checkbox"/></td> <td><span>SERVER_1</span></td> </tr> <tr> <td>3</td> <td><input checked="" type="checkbox"/></td> <td><span>SERVER_1</span></td> <td>7</td> <td><input type="checkbox"/></td> <td><span>SERVER_1</span></td> </tr> <tr> <td>4</td> <td><input checked="" type="checkbox"/></td> <td><span>SERVER_2</span></td> <td>8</td> <td><input type="checkbox"/></td> <td><span>SERVER_1</span></td> </tr> </tbody> </table> |                                     |                       |        |                          |                       | Index | Active | Profile | Index | Active | Profile | 1 | <input type="checkbox"/> | VoIP_SSID | 5 | <input type="checkbox"/> | <span>SERVER_1</span> | 2 | <input type="checkbox"/> | Guest_SSID | 6 | <input type="checkbox"/> | <span>SERVER_1</span> | 3 | <input checked="" type="checkbox"/> | <span>SERVER_1</span> | 7 | <input type="checkbox"/> | <span>SERVER_1</span> | 4 | <input checked="" type="checkbox"/> | <span>SERVER_2</span> | 8 | <input type="checkbox"/> | <span>SERVER_1</span> |
| Index   | Active                              | Profile               | Index  | Active                   | Profile               |       |        |         |       |        |         |   |                          |           |   |                          |                       |   |                          |            |   |                          |                       |   |                                     |                       |   |                          |                       |   |                                     |                       |   |                          |                       |
| 1   | <input type="checkbox"/>            | VoIP_SSID             | 5      | <input type="checkbox"/> | <span>SERVER_1</span> |       |        |         |       |        |         |   |                          |           |   |                          |                       |   |                          |            |   |                          |                       |   |                                     |                       |   |                          |                       |   |                                     |                       |   |                          |                       |
| 2   | <input type="checkbox"/>            | Guest_SSID            | 6      | <input type="checkbox"/> | <span>SERVER_1</span> |       |        |         |       |        |         |   |                          |           |   |                          |                       |   |                          |            |   |                          |                       |   |                                     |                       |   |                          |                       |   |                                     |                       |   |                          |                       |
| 3   | <input checked="" type="checkbox"/> | <span>SERVER_1</span> | 7      | <input type="checkbox"/> | <span>SERVER_1</span> |       |        |         |       |        |         |   |                          |           |   |                          |                       |   |                          |            |   |                          |                       |   |                                     |                       |   |                          |                       |   |                                     |                       |   |                          |                       |
| 4   | <input checked="" type="checkbox"/> | <span>SERVER_2</span> | 8      | <input type="checkbox"/> | <span>SERVER_1</span> |       |        |         |       |        |         |   |                          |           |   |                          |                       |   |                          |            |   |                          |                       |   |                                     |                       |   |                          |                       |   |                                     |                       |   |                          |                       |

- 2 Next, click the **SSID** tab. Check that each configured SSID profile uses the correct **Security**, **Layer-2 Isolation** and **MAC Filter** profiles, as shown in the following figure.

**Figure 41** Tutorial: SSID Tab Correct Settings

| Wireless | SSID  | Security     | RADIUS  | Layer-2 Isolation | MAC Filter |      |                   |                    |
|----------|-------|--------------|---------|-------------------|------------|------|-------------------|--------------------|
|          | Index | Profile Name | SSID    | Security          | RADIUS     | QoS  | Layer-2 Isolation | MAC Filter         |
|          | 1     | VoIP_SSID    | ZyXEL01 | security01        | radius01   | VoIP | Disable           | Disable            |
|          | 2     | Guest_SSID   | ZyXEL02 | security01        | radius01   | NONE | L2isolation01     | Disable            |
|          | 3     | SERVER_1     | SSID_S1 | security03        | radius01   | NONE | L2-ISO_SERVER_1   | MacFilter_SERVER_1 |
|          | 4     | SERVER_2     | SSID_S2 | security04        | radius01   | NONE | L2-ISO_SERVER_2   | MacFilter_SERVER_2 |
|          | 5     | SSID05       | ZyXEL05 | security01        | radius01   | NONE | Disable           | Disable            |
|          | 6     | SSID06       | ZyXEL06 | security01        | radius01   | NONE | Disable           | Disable            |
|          | 7     | SSID07       | ZyXEL07 | security01        | radius01   | NONE | Disable           | Disable            |



If the settings are not as shown, follow the steps in the relevant section of this tutorial again.

#### 4.4.6.2 Testing the Configuration

Before you allow employees to use the network, you need to thoroughly test whether the setup behaves as it should. Take the following steps to do this.

- 1 Test the **SERVER\_1** network.
  - Using Alice's computer and wireless client, and the correct security settings, do the following.
    - Attempt to access Server 1. You should be able to do so.

Attempt to access the Internet. You should be able to do so.

Attempt to access Server **2**. You should be unable to do so. If you can do so, layer-2 isolation is misconfigured.

- Using Alice's computer and wireless client, and incorrect security settings, attempt to associate with the **SERVER\_1** network. You should be unable to do so. If you can do so, security is misconfigured.
- Using another computer and wireless client, but with the correct security settings, attempt to associate with the **SERVER\_1** network. You should be unable to do so. If you can do so, MAC filtering is misconfigured.

**2** Test the **SERVER\_2** network.

- Using Bob's computer and wireless client, and the correct security settings, do the following.

Attempt to access Server **2**. You should be able to do so.

Attempt to access the Internet. You should be able to do so.

Attempt to access Server **1**. You should be unable to do so. If you can do so, layer-2 isolation is misconfigured.

- Using Bob's computer and wireless client, and incorrect security settings, attempt to associate with the **SERVER\_2** network. You should be unable to do so. If you can do so, security is misconfigured.
- Using another computer and wireless client, but with the correct security settings, attempt to associate with the **SERVER\_2** network. You should be unable to do so. If you can do so, MAC filtering is misconfigured.

If you cannot do something that you should be able to do, check the settings as described in [Section 4.4.6.1 on page 74](#), and in the individual Security, layer-2 isolation and MAC filter profiles for the relevant network. If this does not help, see the Troubleshooting chapter in this User's Guide.

---

# PART II

## The Web Configurator

---

System Screens (79)  
Wireless Configuration (85)  
Wireless Security Configuration (101)  
MBSSID and SSID (113)  
Other Wireless Configuration (121)  
IP Screen (133)  
Rogue AP (137)  
Remote Management Screens (143)  
Internal RADIUS Server (161)  
Certificates (169)  
Log Screens (187)  
VLAN (195)  
Maintenance (213)



# System Screens

## 5.1 System Overview

This section provides information on general system setup.

## 5.2 Configuring General Setup

Click **SYSTEM > General**.

**Figure 42** System > General

The following table describes the labels in this screen.

**Table 9** System > General

| LABEL                          | DESCRIPTION  |
|--------------------------------|--|
| General Setup                  |  |
| System Name                    | Type a descriptive name to identify the ZyXEL Device in the Ethernet network. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.   |
| Domain Name                    | This is not a required field. Leave this field blank or enter the domain name here if you know it.   |
| Administrator Inactivity Timer | Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended). |

**Table 9** System > General

| LABEL   | DESCRIPTION  |
|---|--|
| System DNS Servers  |  |
| First DNS Server<br>Second DNS Server<br>Third DNS Server | <p>Select <b>From DHCP</b> if your DHCP server dynamically assigns DNS server information (and the ZyXEL Device's Ethernet IP address). The field to the right displays the (read-only) DNS server IP address that the DHCP assigns.</p> <p>Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b>, but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>. If you set a second choice to <b>User-Defined</b>, and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.</p> <p>The default setting is <b>None</b>.</p> |
| Apply   | Click <b>Apply</b> to save your changes.   |
| Reset   | Click <b>Reset</b> to reload the previous configuration for this screen.   |

## 5.3 Administrator Authentication on RADIUS

The administrator authentication on RADIUS feature lets a (external or internal) RADIUS server authenticate management logins to the ZyXEL Device. This is useful if you need to regularly change a password that you use to manage several ZyXEL Devices.

Activate administrator authentication on RADIUS in the **SYSTEM > Password** screen and configure the same user name, password and RADIUS server information on each ZyXEL Device. Then, whenever you want to change the password, just change it on the RADIUS server.

### 5.3.1 Configuring the Password

It is strongly recommended that you change your ZyXEL Device's password. Click **SYSTEM > Password**. The screen appears as shown.

If you forget your ZyXEL Device's password (or IP address), you will need to reset the device. See the section on resetting the ZyXEL Device for details



Regardless of how you configure this screen, you still use the local system password to log in via the console port (for internal use only).

**Figure 43** SYSTEM > Password.

The following table describes the labels in this screen.

**Table 10** Password

| LABEL                  | DESCRIPTIONS  |
|------------------------|---|
| Enable Admin at Local  | Select this check box to have the device authenticate management logins to the device.  |
| Use old setting        | Select this to have the ZyXEL Device use the local management password already configured on the device ("1234" is the default).  |
| Use new setting        | Select this if you want to change the local management password.  |
| Old Password           | Type in your existing system password ("1234" is the default password).   |
| New Password           | Type your new system password (up to 31 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.   |
| Retype to Confirm      | Retype your new system password for confirmation.   |
| Enable Admin on RADIUS | Select this (and configure the other fields in this section) to have a RADIUS server authenticate management logins to the ZyXEL Device.  |
| Use old setting        | Select this to have a RADIUS server authenticate management logins to the ZyXEL Device using the RADIUS username and password already configured on the device.   |
| Use new setting        | Select this if you want to change the RADIUS username and password the ZyXEL Device uses to authenticate management logon.  |
| User Name              | Enter the username for this user account. This name can be up to 31 ASCII characters long, including spaces.  |
| Password               | Type a password (up to 31 ASCII characters) for this user profile. Note that as you type a password, the screen displays a (*) for each character you type. Spaces are allowed.<br><br>Note: If you are using PEAP authentication, this password field is limited to 14 ASCII characters in length. |

**Table 10** Password

| LABEL  | DESCRIPTIONS  |
|--------|---|
| RADIUS | <p>Select the RADIUS server profile of the RADIUS server that is to authenticate management logins to the ZyXEL Device.</p> <p>The ZyXEL Device tests the user name and password against the RADIUS server when you apply your settings.</p> <ul style="list-style-type: none"> <li>The user name and password must already be configured in the RADIUS server.</li> <li>You must already have a RADIUS profile configured for the RADIUS server (see <a href="#">Section 7.5 on page 111</a>).</li> <li>The server must be set to <b>Active</b> in the profile.</li> </ul> |
| Apply  | Click <b>Apply</b> to save your changes.  |
| Reset  | Click <b>Reset</b> to reload the previous configuration for this screen.  |

## 5.4 Configuring Time Setting

To change your ZyXEL Device's time and date, click **SYSTEM > Time Setting**. The screen appears as shown. Use this screen to configure the ZyXEL Device's time based on your local time zone.

**Figure 44** SYSTEM > Time Setting

The screenshot displays the 'SYSTEM > Time Setting' configuration interface. It features three tabs: 'General', 'Password', and 'Time Setting'. The 'Time Setting' tab is active, showing the following sections:

- Current Time and Date:** Displays 'Current Time' as 00:33:4 and 'Current Date' as 2000-01-01.
- Time and Date Setup:** Includes radio buttons for 'Manual' (selected), 'Get from Time Server' (with sub-options 'Auto' and 'User Defined Time Server Address'), and 'Time Zone Setup' (with a dropdown menu showing '(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London').
- Daylight Savings:** A section with checkboxes and date/time pickers for 'Start Date' and 'End Date', both set to 'First Sunday of January (2000-01-02) at 0 o'clock'.

At the bottom of the screen, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

**Table 11** SYSTEM > Time Setting

| LABEL                               | DESCRIPTION  |
|-------------------------------------|--|
| Current Time                        | This field displays the time of your ZyXEL Device.<br>Each time you reload this page, the ZyXEL Device synchronizes the time with the time server (if configured).   |
| Current Date                        | This field displays the last updated date from the time server.  |
| Manual                              | Select this radio button to enter the time and date manually. If you configure a new time and date, time zone and daylight saving at the same time, the time zone and daylight saving will affect the new time and date you entered.   |
| New Time<br>(hh:mm:ss)              | This field displays the last updated time from the time server or the last time configured manually.<br>When you set <b>Time and Date Setup</b> to <b>Manual</b> , enter the new time in this field and then click <b>Apply</b> .  |
| New Date<br>(yyyy:mm:dd)            | This field displays the last updated date from the time server or the last date configured manually.<br>When you set <b>Time and Date Setup</b> to <b>Manual</b> , enter the new date in this field and then click <b>Apply</b> .  |
| Get from Time Server                | Select this radio button to have the ZyXEL Device get the time and date from the time server you specify below.  |
| Auto                                | Select this to have the ZyXEL Device use the predefined list of time servers.  |
| User Defined Time<br>Server Address | Enter the IP address or URL of your time server. Check with your ISP/ network administrator if you are unsure of this information.   |
| Time Zone                           | Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).   |
| Daylight Savings                    | Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.   |
| Start Date                          | Configure the day and time when Daylight Saving Time starts if you selected <b>Daylight Savings</b> . The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples:<br><br>Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>Second, Sunday, March</b> and type 2 in the <b>o'clock</b> field.<br><br>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Mar., Last, Sun</b> . The time you type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type "02" because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| End Date                            | Configure the day and time when Daylight Saving Time ends if you selected <b>Daylight Savings</b> . The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples:<br><br>Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>First, Sunday, November</b> and type 2 in the <b>o'clock</b> field.<br><br>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Oct., Last, Sun</b> . The time you type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type 02 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).                   |

**Table 11** SYSTEM > Time Setting

| LABEL | DESCRIPTION  |
|-------|--|
| Apply | Click <b>Apply</b> to save your changes.                                 |
| Reset | Click <b>Reset</b> to reload the previous configuration for this screen. |

## 5.5 Pre-defined NTP Time Servers List

When you turn on the ZyXEL Device for the first time, the date and time start at 2000-01-01 00:00:00. When you select **Auto** in the **SYSTEM > Time Setting** screen, the ZyXEL Device then attempts to synchronize with one of the following pre-defined list of NTP time servers.

The ZyXEL Device continues to use the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

**Table 12** Default Time Servers

|                     |
|---------------------|
| ntp1.cs.wisc.edu    |
| ntp1.gbg.netnod.se  |
| ntp2.cs.wisc.edu    |
| tock.usno.navy.mil  |
| ntp3.cs.wisc.edu    |
| ntp.cs.strath.ac.uk |
| ntp1.sp.se          |
| time1.stupi.se      |
| tick.stdtime.gov.tw |
| tock.stdtime.gov.tw |
| time.stdtime.gov.tw |

When the ZyXEL Device uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the ZyXEL Device goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

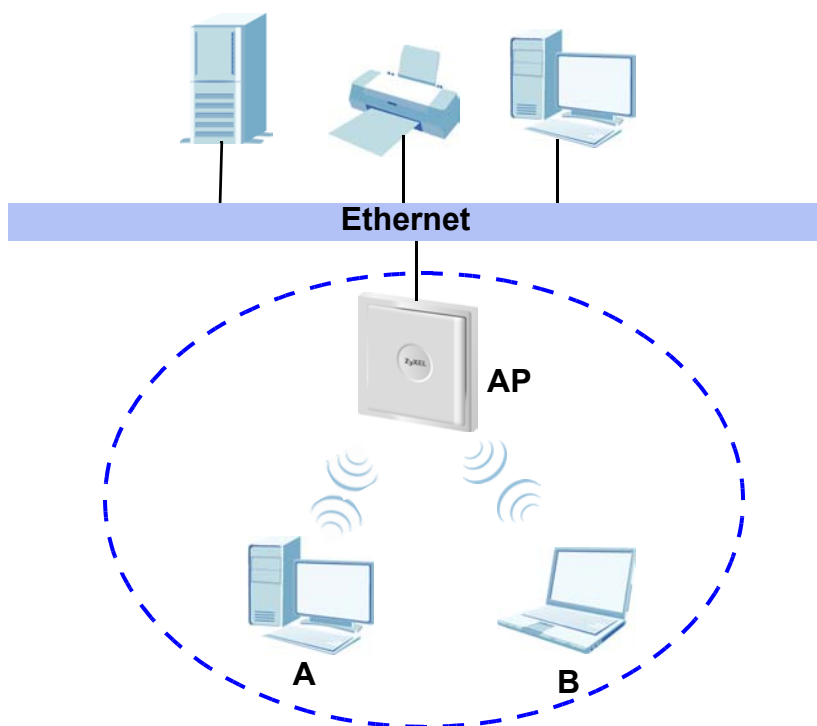
# Wireless Configuration

This chapter discusses how to configure the ZyXEL Device's **Wireless** screens.

## 6.1 Wireless Network Overview

The following figure provides an example of a wireless network.

**Figure 45** Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your ZyXEL Device is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.  
The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use a different channel.

Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every device in the same wireless network must use security compatible with the AP. Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

## 6.2 Wireless LAN Basics

See the Wireless LANs Appendix for information on the following:

- Wireless LAN Topologies
- Channel
- RTS/CTS
- Fragmentation Threshold
- IEEE 802.1x
- RADIUS
- Types of Authentication
- WPA
- Security Parameters Summary

## 6.3 Quality of Service

This section discusses the Quality of Service (QoS) features available on the ZyXEL Device.

### 6.3.1 WMM QoS

WMM (Wi-Fi MultiMedia) QoS (Quality of Service) ensures quality of service in wireless networks. It controls WLAN transmission priority on packets to be transmitted over the wireless network.

WMM QoS prioritizes wireless traffic according to the delivery requirements of the individual and applications. WMM QoS is a part of the IEEE 802.11e QoS enhancement to certified Wi-Fi wireless networks.

On APs without WMM QoS, all traffic streams are given the same access priority to the wireless network. If the introduction of another traffic stream creates a data transmission demand that exceeds the current network capacity, then the new traffic stream reduces the throughput of the other traffic streams.

The ZyXEL Device uses WMM QoS to prioritize traffic streams according to the IEEE 802.1p or DSCP information in each packet's header. The ZyXEL Device automatically determines the priority to use for an individual traffic stream. This prevents reductions in data transmission for applications that are sensitive to latency and jitter (variations in delay).

### 6.3.1.1 WMM QoS Priorities

The following table describes the WMM QoS priority levels that the ZyXEL Device uses.

**Table 13** WMM QoS Priorities

| PRIORITY LEVEL                   | DESCRIPTION   |
|----------------------------------|---|
| voice<br>(WMM_VOICE)             | Typically used for traffic that is especially sensitive to jitter. Use this priority to reduce latency for improved voice quality.  |
| video<br>(WMM_VIDEO)             | Typically used for traffic which has some tolerance for jitter but needs to be prioritized over other data traffic.   |
| best effort<br>(WMM_BEST_EFFORT) | Typically used for traffic from applications or devices that lack QoS capabilities. Use best effort priority for traffic that is less sensitive to latency, but is affected by long delays, such as Internet surfing.   |
| background<br>(WMM_BACKGROUND)   | This is typically used for non-critical traffic such as bulk transfers and print jobs that are allowed but that should not affect other applications and users. Use background priority for applications that do not have strict latency and throughput requirements. |

### 6.3.2 ATC

Automatic Traffic Classifier (ATC) is a bandwidth management tool that prioritizes data packets sent across the network. ATC assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency and a low level of jitter such as Voice over IP or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

ATC assigns priority based on packet size, since time-sensitive applications such as Internet telephony (Voice over IP or VoIP) tend to have smaller packet sizes than non-time sensitive applications such as FTP (File Transfer Protocol). The following table shows some common applications, their time sensitivity, and their typical data packet sizes. Note that the figures given are merely examples - sizes may differ according to application and circumstances.

**Table 14** Typical Packet Sizes

| APPLICATION         | TIME SENSITIVITY | TYPICAL PACKET SIZE (BYTES) |
|---------------------|------------------|-----------------------------|
| Voice over IP (SIP) | High             | < 250                       |
| Online Gaming       | High             | 60 ~ 90                     |
| Web browsing (http) | Medium           | 300 ~ 600                   |
| FTP                 | Low              | 1500                        |

When ATC is activated, the device sends traffic with smaller packets before traffic with larger packets if the network is congested.

ATC assigns priority to packets as shown in the following table.

**Table 15** Automatic Traffic Classifier Priorities

| PACKET SIZE (BYTES) | ATC PRIORITY |
|---------------------|--------------|
| 1 ~ 250             | ATC_High     |
| 250 ~ 1100          | ATC_Medium   |
| 1100 +              | ATC_Low      |

You should activate ATC on the ZyXEL Device if your wireless network includes networking devices that do not support WMM QoS, or if you want to prioritize traffic but do not want to configure WMM QoS settings.

### 6.3.3 ATC+WMM

The ZyXEL Device can use a mapping mechanism to use both ATC and WMM QoS. The ATC+WMM function prioritizes all packets transmitted onto the wireless network using WMM QoS, and prioritizes all packets transmitted onto the wired network using ATC. See [Section 8.2.2 on page 118](#) for details of how to configure ATC+WMM.

Use the ATC+WMM function if you want to do the following:

- enable WMM QoS on your wireless network and automatically assign a WMM priority to packets that do not already have one (see [Section 6.3.3.1 on page 88](#)).
- automatically prioritize all packets going from your wireless network to the wired network (see [Section 6.3.3.2 on page 88](#)).

#### 6.3.3.1 ATC+WMM from LAN to WLAN

ATC+WMM from LAN (the wired Local Area Network) to WLAN (the Wireless Local Area Network) allows WMM prioritization of packets that do not already have WMM QoS priorities assigned. The ZyXEL Device automatically classifies data packets using ATC and then assigns WMM priorities based on that ATC classification.

The following table shows how priorities are assigned for packets coming from the LAN to the WLAN.

**Table 16** ATC + WMM Priority Assignment (LAN to WLAN)

| PACKET SIZE (BYTES) | → | ATC VALUE  | → | WMM VALUE       |
|---------------------|---|------------|---|-----------------|
| 1 ~ 250             |   | ATC_High   |   | WMM_VIDEO       |
| 250 ~ 1100          |   | ATC_Medium |   | WMM_BEST_EFFORT |
| 1100 +              |   | ATC_Low    |   | WMM_BACKGROUND  |

#### 6.3.3.2 ATC+WMM from WLAN to LAN

ATC+WMM from WLAN to LAN automatically prioritizes (assigns an ATC value to) all packets coming from the WLAN. Packets are assigned an ATC value based on their WMM value, not their size.

The following table shows how priorities are assigned for packets coming from the WLAN to the LAN when using ATC+WMM.

**Table 17** ATC + WMM Priority Assignment (WLAN to LAN)

| WMM VALUE       | → | ATC VALUE  |
|-----------------|---|------------|
| WMM_VOICE       |   | ATC_High   |
| WMM_VIDEO       |   | ATC_High   |
| WMM_BEST_EFFORT |   | ATC_Medium |
| WMM_BACKGROUND  |   | ATC_Low    |
| NONE            |   | ATC_Medium |

### 6.3.4 Type Of Service (ToS)

Network traffic can be classified by setting the ToS (Type Of Service) values at the data source (for example, at the ZyXEL Device) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

#### 6.3.4.1 DiffServ

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

#### 6.3.4.2 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

**Figure 46** DiffServ: Differentiated Service Field

|                 |                   |
|-----------------|-------------------|
| DSCP<br>(6-bit) | Unused<br>(2-bit) |
|-----------------|-------------------|

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

### 6.3.5 ToS (Type of Service) and WMM QoS

The DSCP value of outgoing packets is between 0 and 255. 0 is the default priority. WMM QoS checks the DSCP value in the header of data packets. It gives the traffic a priority according to this number.

In order to control which priority level is given to traffic, the device sending the traffic must set the DSCP value in the header. If the DSCP value is not specified, then the traffic is treated as best-effort. This means the wireless clients and the devices with which they are communicating must both set the DSCP value in order to make the best use of WMM QoS. A Voice over IP (VoIP) device for example may allow you to define the DSCP value.

The following table lists which WMM QoS priority level the ZyXEL Device uses for specific DSCP values.

**Table 18** ToS and IEEE 802.1d to WMM QoS Priority Level Mapping

| DSCP VALUE         | WMM QOS PRIORITY LEVEL |
|--------------------|------------------------|
| 224, 192           | voice                  |
| 160, 128           | video                  |
| 96, 0 <sup>A</sup> | besteffort             |
| 64, 32             | background             |

A. The ZyXEL Device also uses best effort for any DSCP value for which another WMM QoS priority is not specified (255, 158 or 37 for example).

## 6.4 Spanning Tree Protocol (STP)

STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other STP-compliant bridges in your network to ensure that only one route exists between any two stations on the network.

### 6.4.1 Rapid STP

The ZyXEL Device uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allow faster convergence of the spanning tree (while also being backwards compatible with STP-only aware bridges). Using RSTP topology change information does not have to propagate to the root bridge and unwanted learned addresses are flushed from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

### 6.4.2 STP Terminology

The root bridge is the base of the spanning tree; it is the bridge with the lowest identifier value (MAC address).

Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost - see the following table.

**Table 19** STP Path Costs

|           | LINK SPEED | RECOMMENDED VALUE | RECOMMENDED RANGE | ALLOWED RANGE |
|-----------|------------|-------------------|-------------------|---------------|
| Path Cost | 4Mbps      | 250               | 100 to 1000       | 1 to 65535    |
| Path Cost | 10Mbps     | 100               | 50 to 600         | 1 to 65535    |
| Path Cost | 16Mbps     | 62                | 40 to 400         | 1 to 65535    |
| Path Cost | 100Mbps    | 19                | 10 to 60          | 1 to 65535    |
| Path Cost | 1Gbps      | 4                 | 3 to 10           | 1 to 65535    |
| Path Cost | 10Gbps     | 2                 | 1 to 5            | 1 to 65535    |

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this bridge has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

### 6.4.3 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware bridges exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

### 6.4.4 STP Port States

STP assigns five port states (see next table) to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

**Table 20** STP Port States

| PORT STATES | DESCRIPTIONS  |
|-------------|---|
| Disabled    | STP is disabled (default).  |
| Blocking    | Only configuration and management BPDUs are received and processed.   |
| Listening   | All BPDUs are received and processed.   |
| Learning    | All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded. |
| Forwarding  | All BPDUs are received and processed. All information frames are received and forwarded.                          |

## 6.5 DFS

When you choose **802.11a** in **Access Point** mode, the ZyXEL Device uses DFS (Dynamic Frequency Selection) to give you a wider choice of wireless channels.

DFS allows you to use channels in the frequency range normally reserved for radar systems. Radar uses radio signals to detect the location of objects for military, meteorological or air traffic control purposes. As long as your ZyXEL Device detects no radar activity on the channel you select, you can use the channel to communicate. However, a wireless LAN operating on the same frequency as an active radar system could disrupt the radar system. Therefore, if the ZyXEL Device detects radar activity on the channel you select, it automatically instructs the wireless clients to move to another channel, then resumes communications on the new channel.

## 6.6 Wireless Screen Overview

The following is a list of the wireless screens you can configure on the ZyXEL Device.

| Wireless | SSID | Security | RADIUS | Layer-2 Isolation | MAC Filter |
|----------|------|----------|--------|-------------------|------------|
|----------|------|----------|--------|-------------------|------------|

- 1 Configure the ZyXEL Device to operate in AP, Bridge/Repeater, AP+Bridge or MBSSID mode in the **Wireless** screen. You can also select an **SSID Profile** in the **Wireless** screen.
- 2 Use the **SSID** screens to view and edit SSID profiles.
- 3 Use the **Security** screen to configure wireless security profiles.
- 4 Use the **RADIUS** screen to configure RADIUS authentication and accounting settings.
- 5 Use the **Layer-2 Isolation** screen to prevent wireless clients associated with your ZyXEL Device from communicating with other wireless clients, APs, computers or routers in a network.
- 6 Use the **MAC Filter** screen to allow or restrict access to your wireless network based on a client's MAC address.

## 6.7 Configuring Wireless Settings

Click **WIRELESS > Wireless**. The screen varies depending upon the operating mode you select.

### 6.7.1 Access Point Mode

Select **Access Point** as the **Operating Mode** to display the screen shown next.

**Figure 47** Wireless: Access Point

| Wireless  | SSID | Security | RADIUS | Layer-2 Isolation | MAC Filter |
|---|------|----------|--------|-------------------|------------|
| <div> <div>WLAN Interface</div> <div>WLAN1</div> </div>   |      |          |        |                   |            |
| <div> <div>Operating Mode</div> <div>Access Point</div> </div>  |      |          |        |                   |            |
| <div> <div>802.11 Mode</div> <div>802.11b+g</div> </div>  |      |          |        |                   |            |
| <div> <input checked="" type="checkbox"/> Super Mode         </div>   |      |          |        |                   |            |
| <div> <div>Choose Channel ID</div> <div>Channel-06 2437MHz</div> <div>or</div> <div>Scan</div> </div>                                     |      |          |        |                   |            |
| <div> <div>RTS/CTS Threshold</div> <div>2346</div> <div>(256 ~ 2346)</div> </div>   |      |          |        |                   |            |
| <div> <div>Fragmentation Threshold</div> <div>2346</div> <div>(256 ~ 2346) (Fragmentation threshold shall be an even number)</div> </div> |      |          |        |                   |            |
| <div> <div>Output Power</div> <div>100%</div> </div>  |      |          |        |                   |            |
| <div> <div>SSID Profile</div> <div>SSID03</div> </div>  |      |          |        |                   |            |
| <div> <input checked="" type="checkbox"/> Enable Spanning Tree Protocol (STP)         </div>  |      |          |        |                   |            |
| <div> <input checked="" type="checkbox"/> Enable Roaming         </div>   |      |          |        |                   |            |
| <div> <small>(The STP and Roaming are common settings. The changes are for both WLAN Interfaces.)</small> </div>                          |      |          |        |                   |            |
| <div> <div>Apply</div> <div>Reset</div> </div>  |      |          |        |                   |            |

The following table describes the general wireless LAN labels in this screen.

**Table 21** Wireless: Access Point

| LABEL                             | DESCRIPTION  |
|-----------------------------------|--|
| WLAN Interface                    | Select which WLAN adapter you want to configure.<br>It is recommended that you configure the first WLAN adapter for AP functions and use the second WLAN adapter for bridge functions.   |
| Operating Mode                    | Select <b>Access Point</b> from the drop-down list.  |
| 802.11 Mode                       | Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device.<br>Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device.<br>Select <b>802.11b+g</b> to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.<br>Select <b>802.11a</b> to allow only IEEE 802.11a compliant WLAN devices to associate with the ZyXEL Device. |
| Super Mode                        | Select this to improve data throughput on the WLAN by enabling fast frame and packet bursting.   |
| Choose Channel ID                 | Set the operating frequency/channel depending on your particular region.<br>To manually set the ZyXEL Device to use a channel, select a channel from the drop-down list box.<br>Click <b>MAINTENANCE</b> and then the <b>Channel Usage</b> tab to open the <b>Channel Usage</b> screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network.<br>To have the ZyXEL Device automatically select a channel, click <b>Scan</b> instead.   |
| Scan                              | Click this button to have the ZyXEL Device automatically scan for and select the channel with the least interference.  |
| Disable channel switching for DFS | This field is available when you select <b>802.11a</b> in the <b>802.11 Mode</b> field.<br>DFS (dynamic frequency selection) allows an AP to detect other devices in the same channel. If there is another device using the same channel, the AP changes to a different channel, so that it can avoid interference with radar systems or other wireless networks.<br>Select this option to disable DFS on the ZyXEL Device when <b>802.11 Mode</b> is set to <b>802.11a</b> .  |
| RTS/CTS Threshold                 | The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to its smallest value (256) turns on the RTS/CTS handshake. Enter a value between <b>256</b> and <b>2346</b> .<br>This field is not available when <b>Super Mode</b> is selected.   |
| Fragmentation Threshold           | The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between <b>256</b> and <b>2346</b> .<br>This field is not available when <b>Super Mode</b> is selected.  |
| Output Power                      | Set the output power of the ZyXEL Device in this field. If there is a high density of APs in an area, decrease the output power of the ZyXEL Device to reduce interference with other APs. Select one of the following <b>100%</b> , <b>50%</b> , <b>25%</b> , <b>12.5%</b> or <b>Minimum</b> . See the product specifications for more information on your ZyXEL Device's output power.<br>This field is not available when you select <b>802.11a</b> in the <b>802.11 Mode</b> field.  |

**Table 21** Wireless: Access Point

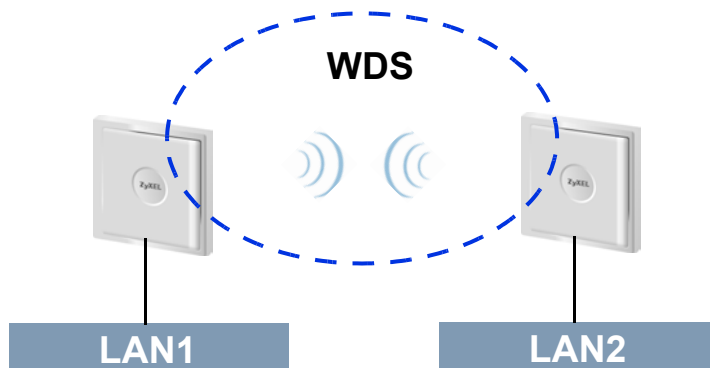
| LABEL                              | DESCRIPTION   |
|------------------------------------|---|
| SSID Profile                       | <p>The SSID (Service Set Identifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Select an <b>SSID Profile</b> from the drop-down list box.</p> <p>Configure SSID profiles in the <b>SSID</b> screen (see <a href="#">Section 8.2 on page 117</a> for information on configuring SSID).</p> <p><b>Note:</b> If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or security settings, you will lose your wireless connection when you press <b>Apply</b> to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.</p> |
| Enable Spanning Tree Control (STP) | (R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP - compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select this to activate STP on the ZyXEL Device.  |
| Enable Roaming                     | <p>Roaming allows wireless stations to switch from one access point to another as they move from one coverage area to another. Select this to enable roaming on the ZyXEL Device if you have two or more ZyXEL Devices on the same subnet.</p> <p><b>Note:</b> All APs on the same subnet and the wireless stations must have the same SSID to allow roaming.</p>   |
| Apply                              | Click <b>Apply</b> to save your changes.  |
| Reset                              | Click <b>Reset</b> to begin configuring this screen afresh.   |

### 6.7.2 Bridge/Repeater Mode

The ZyXEL Device can act as a wireless network bridge and establish wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode.

The ZyXEL Device can establish up to five wireless links with other APs.

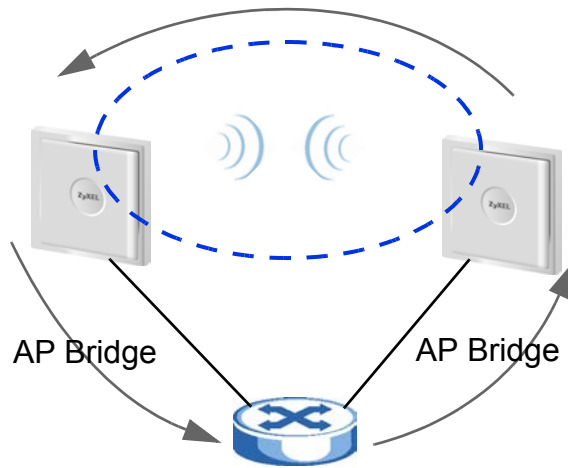
In the example below, when both ZyXEL Devices are in **Bridge/Repeater** mode, they form a WDS (Wireless Distribution System) allowing the computers in **LAN 1** to connect to the computers in **LAN 2**.

**Figure 48** Bridging Example

Be careful to avoid bridge loops when you enable bridging in the ZyXEL Device. Bridge loops cause broadcast traffic to circle the network endlessly, resulting in possible throughput degradation and disruption of communications. The following examples show two network topologies that can lead to this problem:

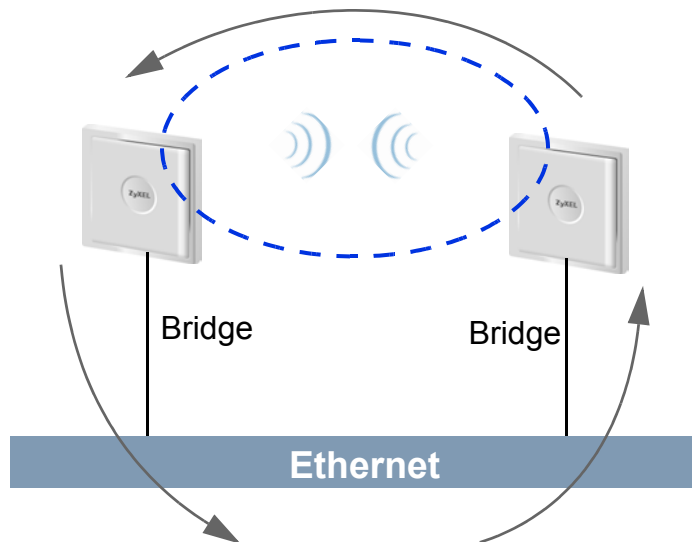
- If two or more ZyXEL Devices (in bridge mode) are connected to the same hub.

**Figure 49** Bridge Loop: Two Bridges Connected to Hub



- If your ZyXEL Device (in bridge mode) is connected to a wired LAN while communicating with another wireless bridge that is also connected to the same wired LAN.

**Figure 50** Bridge Loop: Bridge Connected to Wired LAN



To prevent bridge loops, ensure that you enable STP in the **Wireless** screen or your ZyXEL Device is not set to bridge mode while connected to both wired and wireless segments of the same LAN.

To have the ZyXEL Device act as a wireless bridge only, click **WIRELESS > Wireless** and select **Bridge/Repeater** as the **Operating Mode**.

**Figure 51** Wireless: Bridge/Repeater

**Wireless**

WLAN Interface: WLAN1

Operating Mode: Bridge/Repeater

802.11 Mode: 802.11b+g

Choose Channel ID: Channel-06 2437MHz

RTS/CTS Threshold: 2346 (256 ~ 2346)

Fragmentation Threshold: 2346 (256 ~ 2346) (Fragmentation threshold shall be an even number)

Output Power: 100%

☐ Enable WDS Security

☒ TKIP (ZyAIR Series Compatible)

☐ AES

| Index | Active                   | Remote Bridge MAC | PSK |
|-------|--------------------------|-------------------|-----|
| 1     | <input type="checkbox"/> | 00:00:00:00:00:00 |     |
| 2     | <input type="checkbox"/> | 00:00:00:00:00:00 |     |
| 3     | <input type="checkbox"/> | 00:00:00:00:00:00 |     |
| 4     | <input type="checkbox"/> | 00:00:00:00:00:00 |     |
| 5     | <input type="checkbox"/> | 00:00:00:00:00:00 |     |

☒ Enable Spanning Tree Protocol (STP)  
(The STP and Roaming are common settings. The changes are for both WLAN Interfaces.)

Apply Reset

The following table describes the bridge labels in this screen.

**Table 22** Wireless: Bridge/Repeater

| LABEL             | DESCRIPTIONS   |
|-------------------|--|
| WLAN Interface    | Select which WLAN adapter you want to configure.<br>It is recommended that you configure the first WLAN adapter for AP functions and use the second WLAN adapter for bridge functions.   |
| Operating Mode    | Select <b>Bridge/Repeater</b> in this field.   |
| 802.11 mode       | Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device.<br>Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device.<br>Select <b>802.11b+g</b> to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.<br>Select <b>802.11a</b> to allow only IEEE 802.11a compliant WLAN devices to associate with the ZyXEL Device. |
| Choose Channel ID | Set the operating frequency/channel depending on your particular region.<br>To manually set the ZyXEL Device to use a channel, select a channel from the drop-down list box.<br>Click <b>MAINTENANCE</b> and then the <b>Channel Usage</b> tab to open the <b>Channel Usage</b> screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network.  |

**Table 22** Wireless: Bridge/Repeater

| LABEL                          | DESCRIPTIONS   |
|--------------------------------|--|
| RTS/CTS Threshold              | The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between <b>256</b> and <b>2346</b> .  |
| Fragmentation Threshold        | The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between <b>256</b> and <b>2346</b> .   |
| Output Power                   | Set the output power of the ZyXEL Device in this field. If there is a high density of APs in an area, decrease the output power of the ZyXEL Device to reduce interference with other APs. Select from <b>100%</b> , <b>50%</b> , <b>25%</b> , <b>12.5%</b> and <b>Minimum</b> . See the product specifications for more information on your ZyXEL Device's output power.<br>This field is not available when you select <b>802.11a</b> in the <b>802.11 Mode</b> field.   |
| Enable WDS Security            | Select this to turn on security for the ZyXEL Device's Wireless Distribution System (WDS). A Wireless Distribution System is a wireless connection between two or more APs. If you do not select the check box, traffic between APs is not encrypted.<br><br><b>Note:</b> WDS security is independent of the security settings between the ZyXEL Device and any wireless clients.<br><br>When you enable WDS security, also do the following: <ul style="list-style-type: none"> <li>• Select the type of security you want to use (<b>TKIP</b> or <b>AES</b>) to secure traffic on your WDS.</li> <li>• Enter a pre-shared key in the <b>PSK</b> field for each access point in your WDS. Each access point can use a different pre-shared key.</li> <li>• Configure WDS security and the relevant PSK in each of your other access point(s).</li> </ul> <b>Note:</b> Other APs must use the same encryption method to enable WDS security. |
| TKIP (ZyAIR Series Compatible) | Select this to enable Temporal Key Integrity Protocol (TKIP) security on your WDS. This option is compatible with other ZyXEL access points including that support WDS security. Use this if the other access points on your network support WDS security but do not have an AES option.<br><br><b>Note:</b> Check your other AP's documentation to make sure it supports WDS security.<br><br><b>Note:</b> At the time of writing, this option is compatible with other ZyXEL NWA Series and G-3000/G-3000H access points only.   |
| AES                            | Select this to enable Advanced Encryption System (AES) security on your WDS. AES provides superior security to TKIP. Use AES if the other access points on your network support it for the WDS.<br><br><b>Note:</b> At the time of writing, this option is compatible with other ZyXEL NWA Series access points only.  |
| Index                          | This is the index number of the bridge connection.   |
| Active                         | Select the check box to enable the bridge connection. Otherwise, clear the check box to disable it.  |

**Table 22** Wireless: Bridge/Repeater

| LABEL                     | DESCRIPTIONS  |
|---------------------------|---|
| Remote Bridge MAC Address | Type the MAC address of the peer device in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.  |
| PSK                       | Type a pre-shared key (PSK) from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). You must also set the peer device to use the same pre-shared key. Each peer device can use a different pre-shared key. |

See [Table 21 on page 93](#) for information on the other labels in this screen.

### 6.7.3 AP+Bridge Mode

Select **AP+Bridge** as the **Operating Mode** in the **WIRELESS > Wireless** screen to have the ZyXEL Device function as a bridge and access point simultaneously. See the section on applications for more information.

**Figure 52** Wireless: AP+Bridge

| Wireless  | SSID                     | Security                 | RADIUS     | Layer-2 Isolation | MAC Filter |
|---|--------------------------|--------------------------|------------|-------------------|------------|
| <b>WLAN Interface</b> <span>WLAN1</span>  |                          |                          |            |                   |            |
| <b>Operating Mode</b> <span>AP+Bridge</span>  |                          |                          |            |                   |            |
| <b>802.11 Mode</b> <span>802.11b+g</span>   |                          |                          |            |                   |            |
| <input checked="" type="checkbox"/> <b>Super Mode</b>   |                          |                          |            |                   |            |
| <b>Choose Channel ID</b> <span>Channel-06 2437MHz</span>  |                          |                          |            |                   |            |
| <b>RTS/CTS Threshold</b> <span>2346</span> (256 ~ 2346)   |                          |                          |            |                   |            |
| <b>Fragmentation Threshold</b> <span>2346</span> (256 ~ 2346) (Fragmentation threshold shall be an even number) |                          |                          |            |                   |            |
| <b>Output Power</b> <span>100%</span>   |                          |                          |            |                   |            |
| <b>SSID Profile</b> <span>SSID03</span>   |                          |                          |            |                   |            |
| <input type="checkbox"/> <b>Enable WDS Security</b>   |                          |                          |            |                   |            |
| <input checked="" type="radio"/> <b>TKIP (ZyAIR Series Compatible)</b>  |                          |                          |            |                   |            |
| <input type="radio"/> <b>AES</b>  |                          |                          |            |                   |            |
| <b>Index</b>  | <b>Active</b>            | <b>Remote Bridge MAC</b> | <b>PSK</b> |                   |            |
| 1   | <input type="checkbox"/> | 00:00:00:00:00:00        |            |                   |            |
| 2   | <input type="checkbox"/> | 00:00:00:00:00:00        |            |                   |            |
| 3   | <input type="checkbox"/> | 00:00:00:00:00:00        |            |                   |            |
| 4   | <input type="checkbox"/> | 00:00:00:00:00:00        |            |                   |            |
| 5   | <input type="checkbox"/> | 00:00:00:00:00:00        |            |                   |            |
| <input checked="" type="checkbox"/> <b>Enable Spanning Tree Protocol (STP)</b>                                  |                          |                          |            |                   |            |
| <input type="checkbox"/> <b>Enable Roaming</b>  |                          |                          |            |                   |            |
| <small>(The STP and Roaming are common settings. The changes are for both WLAN Interfaces.)</small>             |                          |                          |            |                   |            |
| <span>Apply</span> <span>Reset</span>   |                          |                          |            |                   |            |

See the tables describing the fields in the **Access Point** and **Bridge/Repeater** operating modes for descriptions of the fields in this screen.

### 6.7.4 MBSSID Mode

Select **MBSSID** as the **Operating Mode**. Refer to [Chapter 8 on page 113](#) for configuration instructions and detailed information. See [Chapter 7 on page 101](#) for details on the security settings.



# Wireless Security Configuration

This chapter describes how to use the **Security** and **RADIUS** screens to configure wireless security on your ZyXEL Device.

## 7.1 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

### 7.1.1 SSID

Normally, the ZyXEL Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the ZyXEL Device does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

### 7.1.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.<sup>1</sup> A MAC address is usually written using twelve hexadecimal characters<sup>2</sup>; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the ZyXEL Device which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

- 
1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
  2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

### 7.1.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before they can use it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.


Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

### 7.1.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See [Section 7.1.3 on page 102](#) for information about this.)

**Table 23** Types of Encryption for Each Type of Authentication

|   | NO AUTHENTICATION | RADIUS SERVER |
|---|-------------------|---------------|
| <b>Weakest</b><br><br><b>Strongest</b> | No Security       | WPA           |
|   | Static WEP        |               |
|   | WPA-PSK           |               |
|   | WPA2-PSK          | WPA2          |

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no security, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the ZyXEL Device and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **WEP** in the wireless network.



It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you use WPA2 or WPA2-PSK in your ZyXEL Device, you can select **WPA2-MIX** or **WPA2-PSK-MIX** to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK-MIX** or **WPA2-MIX** (depending on the type of wireless network login) in the ZyXEL Device.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the same wireless network must have the same key.

## 7.2 Security Modes

The following table describes the security modes you can configure.

**Table 24** Security Modes

| SECURITY MODE    | DESCRIPTION   |
|------------------|---|
| None             | Select this to have no data encryption.   |
| WEP              | Select this to use WEP encryption.  |
| 802.1x-Only      | Select this to use 802.1x authentication with no data encryption.   |
| 802.1x-Static64  | Select this to use 802.1x authentication with a static 64bit WEP key and an authentication server.        |
| 802.1x-Static128 | Select this to use 802.1x authentication with a static 128bit WEP key and an authentication server.       |
| WPA              | Select this to use WPA.   |
| WPA-PSK          | Select this to use WPA with a pre-shared key.   |
| WPA2             | Select this to use WPA2.  |
| WPA2-MIX         | Select this to use either WPA2 or WPA depending on which security mode the wireless client uses.          |
| WPA2-PSK         | Select this to use WPA2 with a pre-shared key.  |
| WPA2-PSK-MIX     | Select this to use either WPA-PSK or WPA2-PSK, depending on which security mode the wireless client uses. |

## 7.3 Configuring Security



The following screens are configurable only in **Access Point**, **AP+Bridge** and **MBSSID** operating modes only.

Use the **Security** screen to create secure profiles. A security profile is a group of configuration settings which can be assigned to an SSID profile in the **SSID** configuration screen.

You can configure up to 16 security profiles.

To change your ZyXEL Device's wireless security settings, click **WIRELESS > Security**.

**Figure 53** Wireless > Security

Wireless










SSID

Security

RADIUS

Layer-2 Isolation

MAC Filter

|   | Index | Profile Name | Security Mode |
|---|-------|--------------|---------------|
|  | 1     | security01   | None          |
|  | 2     | security02   | None          |
|  | 3     | security03   | None          |
|  | 4     | security04   | None          |
|  | 5     | security05   | None          |
|  | 6     | security06   | None          |
|  | 7     | security07   | None          |
|  | 8     | security08   | None          |
|  | 9     | security09   | None          |
|  | 10    | security10   | None          |
|  | 11    | security11   | None          |
|  | 12    | security12   | None          |
|  | 13    | security13   | None          |
|  | 14    | security14   | None          |
|  | 15    | security15   | None          |
|  | 16    | security16   | None          |

Edit

The following table describes the labels in this screen.

**Table 25** WIRELESS > Security

| LABEL         | DESCRIPTION  |
|---------------|--|
| Index         | This is the index number of the security profile.  |
| Profile Name  | This field displays a name given to a security profile in the <b>Security</b> configuration screen.  |
| Security Mode | This field displays the security mode this security profile uses.                                    |
| Edit          | Select an entry from the list and click <b>Edit</b> to configure security settings for that profile. |

The next screen varies according to the **Security Mode** you select.

### 7.3.1 Security: WEP

Select **WEP** in the **Security Mode** field to display the following screen.

**Figure 54** WIRELESS > Security: WEP

| Wireless  | SSID | Security | RADIUS | Layer-2 Isolation | MAC Filter |
|---|------|----------|--------|-------------------|------------|
| <b>Profile Name</b> <input type="text" value="security01"/>   |      |          |        |                   |            |
| <b>Security Mode</b> <input type="text" value="WEP"/>   |      |          |        |                   |            |
| <b>WEP Encryption</b> <input type="text" value="64-bit WEP"/>   |      |          |        |                   |            |
| <b>Authentication Method</b> <input type="text" value="Auto"/>  |      |          |        |                   |            |
| <p>64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key (1-4).<br/>           128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key (1-4).<br/>           152-bit WEP: Enter 16 ASCII characters or 32 hexadecimal characters ("0-9", "A-F") for each Key (1-4).</p> |      |          |        |                   |            |
| <input checked="" type="radio"/> ASCII <input type="radio"/> Hex  |      |          |        |                   |            |
| <input checked="" type="radio"/> Key 1 <input type="text"/>   |      |          |        |                   |            |
| <input type="radio"/> Key 2 <input type="text"/>  |      |          |        |                   |            |
| <input type="radio"/> Key 3 <input type="text"/>  |      |          |        |                   |            |
| <input type="radio"/> Key 4 <input type="text"/>  |      |          |        |                   |            |
| <div>Apply</div> <div>Reset</div>   |      |          |        |                   |            |

The following table describes the labels in this screen.

**Table 26** Security: WEP

| LABEL                 | DESCRIPTION  |
|-----------------------|--|
| Profile Name          | Type a name to identify this security profile.   |
| Security Mode         | Choose <b>WEP</b> in this field.   |
| WEP Encryption        | Select <b>64-bit WEP</b> , <b>128-bit WEP</b> or <b>152-bit WEP</b> to enable data encryption.   |
| Authentication Method | Select <b>Auto</b> or <b>Shared Key</b> from the drop-down list box.<br>The default setting is <b>Auto</b> .   |
| ASCII                 | Select this option to enter ASCII characters as the WEP keys.  |
| Hex                   | Select this option to enter hexadecimal characters as the WEP keys.<br>The preceding "0x" is entered automatically.  |
| Key 1 to Key 4        | The WEP keys are used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission.<br>If you chose <b>64-bit WEP</b> , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").<br>If you chose <b>128-bit WEP</b> , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").<br>If you chose <b>152-bit WEP</b> , then enter 16 ASCII characters or 32 hexadecimal characters ("0-9", "A-F").<br>You must configure all four keys, but only one key can be activated at any one time. The default key is key 1. |
| Apply                 | Click <b>Apply</b> to save your changes.   |
| Reset                 | Click <b>Reset</b> to begin configuring this screen afresh.  |

### 7.3.2 Security: 802.1x Only

Select **8021x-Only** in the **Security Mode** field to display the following screen.

**Figure 55** Security: 802.1x Only

| Wireless   | SSID | Security | RADIUS | Layer-2 Isolation | MAC Filter |
|--|------|----------|--------|-------------------|------------|
| <div> <div>Profile Name</div> <div>security01</div> </div> <div> <div>Security Mode</div> <div>8021x-Only</div> </div> <div> <div>ReAuthentication Timer</div> <div>0 (seconds, 0 means no ReAuthentication)</div> </div> <div> <div>Idle Timeout</div> <div>3600 (seconds)</div> </div> |      |          |        |                   |            |
| <div> <div>Apply</div> <div>Reset</div> </div>   |      |          |        |                   |            |

The following table describes the labels in this screen.

**Table 27** Security: 802.1x Only

| LABEL                  | DESCRIPTION   |
|------------------------|---|
| Profile Name           | Type a name to identify this security profile.  |
| Security Mode          | Choose <b>8021x-Only</b> in this field.   |
| ReAuthentication Timer | <p>Specify how often wireless stations have to resend user names and passwords in order to stay connected.</p> <p>Enter a time interval between 10 and 9999 seconds. The default time interval is <b>1800</b> seconds (30 minutes). Alternatively, enter "0" to turn reauthentication off.</p> <p>Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</p> |
| Idle Timeout           | <p>The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed.</p> <p>The default time interval is <b>3600</b> seconds (or 1 hour).</p>  |
| Apply                  | Click <b>Apply</b> to save your changes.  |
| Reset                  | Click <b>Reset</b> to begin configuring this screen afresh.   |

### 7.3.3 Security: 802.1x Static 64-bit, 802.1x Static 128-bit

Select **8021x-Static64** or **8021x-Static128** in the **Security Mode** field to display the following screen.

**Figure 56** Security: 802.1x Static 64-bit, 802.1x Static 128-bit

| Wireless   | SSID | Security | RADIUS | Layer-2 Isolation | MAC Filter |
|--|------|----------|--------|-------------------|------------|
| <b>Profile Name :</b> <input type="text" value="security04"/>  |      |          |        |                   |            |
| <b>Security Mode :</b> <input type="text" value="8021x-Static128"/>  |      |          |        |                   |            |
| Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key (1-4). <div style="text-align: center;"> <input checked="" type="radio"/> ASCII    <input type="radio"/> Hex           </div>   |      |          |        |                   |            |
| <div> <input checked="" type="radio"/> <b>Key 1</b> <input type="radio"/> <b>Key 2</b> <input type="radio"/> <b>Key 3</b> <input type="radio"/> <b>Key 4</b> </div> <div> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> </div> |      |          |        |                   |            |
| <b>ReAuthentication Timer :</b> <input type="text" value="1800"/> ( in seconds, 0 mean no ReAuthentication)  |      |          |        |                   |            |
| <b>Idle Timeout :</b> <input type="text" value="3600"/> ( in seconds)  |      |          |        |                   |            |
| <input type="button" value="Apply"/> <input type="button" value="Reset"/>  |      |          |        |                   |            |

The following table describes the labels in this screen.

**Table 28** Security: 802.1x Static 64-bit, 802.1x Static 128-bit

| LABEL                  | DESCRIPTION   |
|------------------------|---|
| Profile Name           | Type a name to identify this security profile.  |
| Security Mode          | Choose <b>8021x-Static64</b> or <b>8021x-Static128</b> in this field.   |
| ASCII                  | Select this option to enter ASCII characters as the WEP keys.   |
| Hex                    | Select this option to enter hexadecimal characters as the WEP keys.The preceding "0x" is entered automatically.   |
| Key 1 to Key 4         | <p>If you chose <b>802.1x Static 64</b>, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.</p> <p>If you chose <b>802.1x Static 128-bit</b>, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.</p> <p>There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations.</p> <p>The preceding "0x" is entered automatically. You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.</p> |
| ReAuthentication Timer | <p>Specify how often wireless stations have to resend user names and passwords in order to stay connected.</p> <p>Enter a time interval between 10 and 9999 seconds. The default time interval is <b>1800</b> seconds (30 minutes). Alternatively, enter "0" to turn reauthentication off.</p> <p><b>Note:</b> If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</p>  |
| Idle Timeout           | <p>The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed.</p> <p>The default time interval is <b>3600</b> seconds (or 1 hour).</p>  |
| Apply                  | Click <b>Apply</b> to save your changes.  |
| Reset                  | Click <b>Reset</b> to begin configuring this screen afresh.   |

### 7.3.4 Security: WPA

Select **WPA** in the **Security Mode** field to display the following screen.

**Figure 57** Security: WPA

| Wireless   | SSID | Security                                 | RADIUS | Layer-2 Isolation | MAC Filter |
|--|------|--|--------|-------------------|------------|
| Profile Name   |      | security01                               |        |                   |            |
| Security Mode  |      | WPA                                      |        |                   |            |
| ReAuthentication Timer   |      | 0 (seconds, 0 means no ReAuthentication) |        |                   |            |
| Idle Timeout   |      | 3600 (seconds)                           |        |                   |            |
| Group Key Update Timer   |      | 1800 (seconds)                           |        |                   |            |
| <div> <input type="button" value="Apply"/> <input type="button" value="Reset"/> </div> |      |  |        |                   |            |

The following table describes the labels in this screen.

**Table 29** Security: WPA

| LABEL                  | DESCRIPTION  |
|------------------------|--|
| Name                   | Type a name to identify this security profile.   |
| Security Mode          | Choose <b>WPA</b> in this field.   |
| ReAuthentication Timer | Specify how often wireless stations have to resend user names and passwords in order to stay connected.<br>Enter a time interval between 10 and 9999 seconds. The default time interval is <b>1800</b> seconds (30 minutes). Alternatively, enter "0" to turn reauthentication off.<br><br>Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority. |
| Idle Timeout           | The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed.<br>The default time interval is <b>3600</b> seconds (or 1 hour).  |
| Group Key Update Timer | The <b>Group Key Update Timer</b> is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>Group Key Update Timer</b> is also supported in WPA-PSK mode. The ZyXEL Device default is 1800 seconds (30 minutes).                                     |
| Apply                  | Click <b>Apply</b> to save your changes.   |
| Reset                  | Click <b>Reset</b> to begin configuring this screen afresh.  |

### 7.3.5 Security: WPA2 or WPA2-MIX

Select **WPA2** or **WPA2-MIX** in the **Security Mode** field to display the following screen.

**Figure 58** Security:WPA2 or WPA2-MIX

| Wireless   | SSID | Security | RADIUS | Layer-2 Isolation | MAC Filter |
|--|------|----------|--------|-------------------|------------|
| <div> <div>Profile Name</div> <input type="text" value="security01"/> </div> <div> <div>Security Mode</div> <div>WPA2-MIX</div> </div> <div> <div>ReAuthentication Timer</div> <div>0</div> <div>(seconds, 0 means no ReAuthentication)</div> </div> <div> <div>Idle Timeout</div> <div>3600</div> <div>(seconds)</div> </div> <div> <div>Group Key Update Timer</div> <div>1800</div> <div>(seconds)</div> </div> <div> <div>PMK Cache</div> <div>Enable</div> </div> <div> <div>Pre-Authentication</div> <div>Disable</div> </div> |      |          |        |                   |            |
| <div> <div>Apply</div> <div>Reset</div> </div>   |      |          |        |                   |            |

The following table describes the labels not previously discussed

**Table 30** Security: WPA2 or WPA2-MIX

| LABEL                  | DESCRIPTIONS   |
|------------------------|--|
| Profile Name           | Type a name to identify this security profile.   |
| Security Mode          | Choose <b>WPA2</b> or <b>WPA2-MIX</b> in this field.   |
| ReAuthentication Timer | <p>Specify how often wireless stations have to resend usernames and passwords in order to stay connected.</p> <p>Enter a time interval between 10 and 9999 seconds. The default time interval is <b>1800</b> seconds (30 minutes). Alternatively, enter "0" to turn reauthentication off.</p> <p>Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</p>   |
| Idle Timeout           | <p>The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed.</p> <p>The default time interval is <b>3600</b> seconds (or 1 hour).</p>  |
| Group Key Update Timer | <p>The <b>Group Key Update Timer</b> is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>Group Key Update Timer</b> is also supported in WPA-PSK mode. The ZyXEL Device's default is 1800 seconds (30 minutes).</p>  |
| PMK Cache              | <p>When a wireless client moves from one AP's coverage area to another, it performs an authentication procedure (exchanging security information) with the new AP. Instead of re-authenticating a client each time it returns to the AP's coverage area, which can cause delays to time-sensitive applications, the AP and the client can store (or "cache") and use information about their previous authentication. Select <b>Enable</b> to allow PMK caching, or <b>Disable</b> to switch this feature off.</p> |
| Pre-Authentication     | <p>Pre-authentication allows a wireless client to perform authentication with a different AP from the one to which it is currently connected, before moving into the new AP's coverage area. This speeds up roaming. Select <b>Enable</b> to allow pre-authentication, or <b>Disable</b> to switch it off.</p>   |
| Apply                  | Click <b>Apply</b> to save your changes.   |
| Reset                  | Click <b>Reset</b> to begin configuring this screen afresh.  |

### 7.3.6 Security: WPA-PSK, WPA2-PSK, WPA2-PSK-MIX

Select **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK-MIX** in the **Security Mode** field to display the following screen.

**Figure 59** Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX

| Wireless  | SSID | Security | RADIUS | Layer-2 Isolation | MAC Filter |
|---|------|----------|--------|-------------------|------------|
| <div> <div>Profile Name</div> <div>security01</div> </div> <div> <div>Security Mode</div> <div>WPA2-PSK-MIX</div> </div> <div> <div>Pre-Shared Key</div> <div></div> </div> <div> <div>ReAuthentication Timer</div> <div>0</div> <div>(seconds, 0 means no ReAuthentication)</div> </div> <div> <div>Idle Timeout</div> <div>3600</div> <div>(seconds)</div> </div> <div> <div>Group Key Update Timer</div> <div>1800</div> <div>(seconds)</div> </div> |      |          |        |                   |            |
| <div> <div>Apply</div> <div>Reset</div> </div>  |      |          |        |                   |            |

The following table describes the labels not previously discussed

**Table 31** Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX

| LABEL                  | DESCRIPTION   |
|------------------------|---|
| Profile Name           | Type a name to identify this security profile.  |
| Security Mode          | Choose <b>WPA-PSK</b> , <b>WPA2-PSK</b> or <b>WPA2-PSK-MIX</b> in this field.   |
| Pre-Shared Key         | <p>The encryption mechanisms used for <b>WPA</b> and <b>WPA-PSK</b> are the same. The only difference between the two is that <b>WPA-PSK</b> uses a simple common password, instead of user-specific credentials.</p> <p>Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).</p>   |
| ReAuthentication Timer | <p>Specify how often wireless stations have to resend usernames and passwords in order to stay connected.</p> <p>Enter a time interval between 10 and 9999 seconds. The default time interval is <b>1800</b> seconds (30 minutes). Alternatively, enter "0" to turn reauthentication off.</p> <p><b>Note:</b> If wireless station authentication is done using a <b>RADIUS</b> server, the reauthentication timer on the <b>RADIUS</b> server has priority.</p> |
| Idle Timeout           | <p>The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed.</p> <p>The default time interval is <b>3600</b> seconds (or 1 hour).</p>   |
| Group Key Update Timer | <p>The <b>Group Key Update Timer</b> is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>Group Key Update Timer</b> is also supported in WPA-PSK mode. The ZyXEL Device's default is 1800 seconds (30 minutes).</p>   |
| Apply                  | Click <b>Apply</b> to save your changes.  |
| Reset                  | Click <b>Reset</b> to begin configuring this screen afresh.   |

## 7.4 Introduction to RADIUS

RADIUS is based on a client-sever model that supports authentication and accounting, where the access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks, among others:

- Authentication  
Determines the identity of the users.
- Accounting  
Keeps track of the client's network activity.

The ZyXEL Device is equipped with an internal RADIUS server. See [Section 13.1 on page 161](#) for more details.

## 7.5 Configuring RADIUS

Use RADIUS if you want to authenticate wireless users using the internal authentication server (see [Section 13.1 on page 161](#)) or an external server.

You can configure up to four RADIUS server profiles. Each profile also has one backup authentication server and a backup accounting server. These profiles can be assigned to an SSID profile in the **SSID** configuration screen

To set up your ZyXEL Device's RADIUS server settings, click **WIRELESS > RADIUS**. The screen appears as shown.

**Figure 60** RADIUS

| Wireless  | SSID | Security  | RADIUS | Layer-2 Isolation  | MAC Filter |
|---|------|---|--------|--|------------|
| <p>Index : <span>1</span></p> <p>Profile Name : <span>radius01</span></p> |      |   |        |  |            |
|   |      | <p>Primary</p> <p><input type="radio"/> Internal <input checked="" type="radio"/> External</p> <p><input type="checkbox"/> Active</p> |        | <p>Backup</p> <p><input type="radio"/> Internal <input checked="" type="radio"/> External</p> <p><input type="checkbox"/> Active</p> |            |
| RADIUS Option   |      |   |        |  |            |
| RADIUS Server IP Address  |      | <span>0.0.0.0</span>  |        | <span>0.0.0.0</span>   |            |
| RADIUS Server Port  |      | <span>1812</span>   |        | <span>1812</span>  |            |
| Share Secret  |      |   |        |  |            |
|   |      | <input type="checkbox"/> Active   |        | <input type="checkbox"/> Active  |            |
| Accounting Server IP Address  |      | <span>0.0.0.0</span>  |        | <span>0.0.0.0</span>   |            |
| Accounting Server Port  |      | <span>1813</span>   |        | <span>1813</span>  |            |
| Share Secret  |      |   |        |  |            |
| <p>Apply Reset</p>  |      |   |        |  |            |

The following table describes the labels in this screen.

**Table 32 RADIUS**

| LABEL                        | DESCRIPTION   |
|------------------------------|---|
| Index                        | Select the RADIUS profile you want to configure from the drop-down list box.  |
| Profile Name                 | Type a name for the RADIUS profile associated with the <b>Index</b> number above.   |
| Primary                      | Configure the fields below to set up user authentication and accounting.  |
| Backup                       | If the ZyXEL Device cannot communicate with the <b>Primary</b> accounting server, you can have the ZyXEL Device use a <b>Backup</b> RADIUS server. Make sure the <b>Active</b> check boxes are selected if you want to use backup servers. The ZyXEL Device will attempt to communicate three times before using the <b>Backup</b> servers. Requests can be issued from the client interface to use the backup server. The length of time for each authentication is decided by the wireless client or based on the configuration of the <b>ReAuthentication Timer</b> field in the <b>Security</b> screen. |
| RADIUS Option                |   |
| Internal                     | Select this check box to use the ZyXEL Device's internal authentication server. The <b>Active</b> , <b>RADIUS Server IP Address</b> , <b>RADIUS Server Port</b> and <b>Share Secret</b> fields are not available when you use the internal authentication server.   |
| External                     | Select this check box to use an external authentication server. The ZyXEL Device does not use the internal authentication server when this check box is enabled.  |
| Active                       | Select the check box to enable user authentication through an external authentication server. This check box is not available when you select <b>Internal</b> .   |
| RADIUS Server IP Address     | Enter the IP address of the external authentication server in dotted decimal notation. This field is not available when you select <b>Internal</b> .  |
| RADIUS Server Port           | Enter the port number of the external authentication server. The default port number is 1812. You need not change this value unless your network administrator instructs you to do so. This field is not available when you select <b>Internal</b> .  |
| Share Secret                 | Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network. This field is not available when you select <b>Internal</b> .   |
| Active                       | Select the check box to enable user accounting through an external authentication server.   |
| Accounting Server IP Address | Enter the IP address of the external accounting server in dotted decimal notation.  |
| Accounting Server Port       | Enter the port number of the external accounting server. The default port number is 1813. You need not change this value unless your network administrator instructs you to do so with additional information.  |
| Share Secret                 | Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external accounting server and the ZyXEL Device. The key must be the same on the external accounting server and your ZyXEL Device. The key is not sent over the network.   |
| Apply                        | Click <b>Apply</b> to save your changes.  |
| Reset                        | Click <b>Reset</b> to begin configuring this screen afresh.   |

# MBSSID and SSID

This chapter describes how to configure and use your ZyXEL Device's MBSSID mode and configure SSID profiles.

## 8.1 Wireless LAN Infrastructures

See the Wireless LAN chapter for some basic WLAN scenarios and terminology.

### 8.1.1 MBSSID

Traditionally, you needed to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there was also the possibility of channel interference. The ZyXEL Device's MBSSID (Multiple Basic Service Set IDentifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying levels of privilege to different SSIDs.

Wireless stations can use different BSSIDs to associate with the same AP.

### 8.1.2 Notes on Multiple BSS

- There is a maximum number of BSSs allowed on one AP simultaneously.  
On the NWA-3160 and NWA-3163, a maximum of eight simultaneous BSSs are allowed.  
On the NWA-3165, a maximum of four simultaneous BSSs are allowed.
- You must use different WEP keys for different BSSs. If two stations have different BSSIDs (they are in different BSSs), but have the same WEP keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

### 8.1.3 Multiple BSS Example

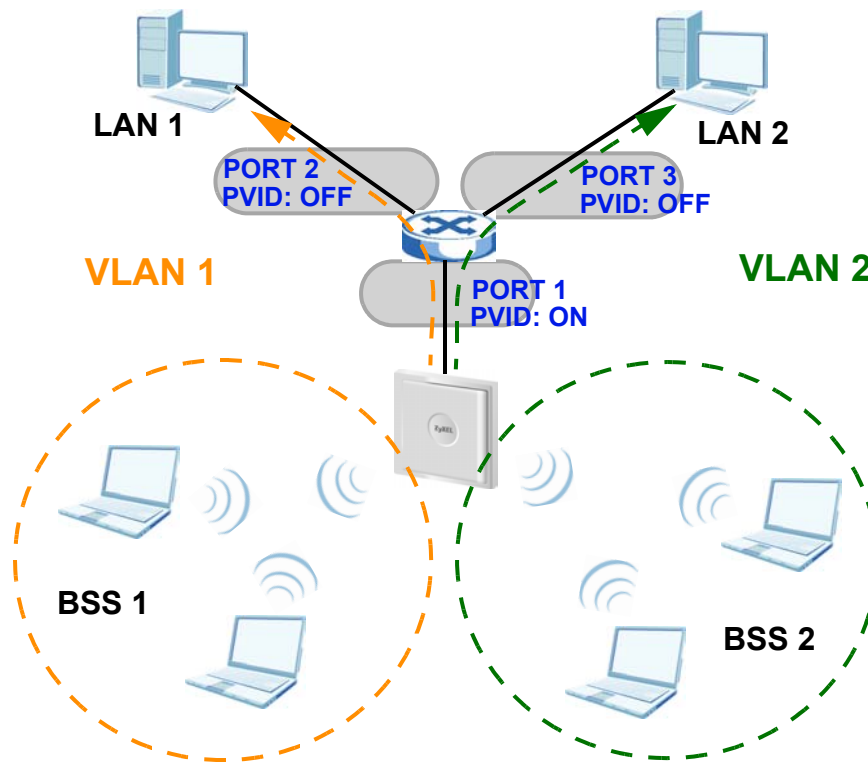
Refer to the applications section for more information.

### 8.1.4 Multiple BSS with VLAN Example

In this example, **VLAN 1** includes the computers in **BSS1** and **LAN 1**. Computers in **BSS2** and **LAN 2** belong to **VLAN 2**. Users in **BSS1** are limited to accessing the resources on **LAN 1** and similarly users in **BSS2** may only access resources on **LAN 2**. **VLAN 2** is the management VLAN.

The switch adds PVID (Port VLAN IDentity) tags to incoming frames that don't already have tags (on switch ports where PVID is enabled).

**Figure 61** Multiple BSS with VLAN Example



### 8.1.5 Configuring Multiple BSSs

Click **WIRELESS > Wireless** and select **MBSSID** in the **Operating Mode** drop-down list box to display the screen as shown.

**Figure 62** Wireless: Multiple BSS

| Wireless  | SSID                     | Security       | RADIUS       | Layer-2 Isolation        | MAC Filter     |
|---|--------------------------|----------------|--------------|--------------------------|----------------|
| <b>WLAN Interface</b> <span>WLAN1</span>  |                          |                |              |                          |                |
| <b>Operating Mode</b> <span>MBSSID</span>   |                          |                |              |                          |                |
| <b>802.11 Mode</b> <span>802.11b+g</span>   |                          |                |              |                          |                |
| <input checked="" type="checkbox"/> <b>Super Mode</b>   |                          |                |              |                          |                |
| <b>Choose Channel ID</b> <span>Channel-06 2437MHz</span> or <span>Scan</span>   |                          |                |              |                          |                |
| <b>RTS/CTS Threshold</b> <span>2346</span> (256 ~ 2346)   |                          |                |              |                          |                |
| <b>Fragmentation Threshold</b> <span>2346</span> (256 ~ 2346) (Fragmentation threshold shall be an even number)   |                          |                |              |                          |                |
| <b>Output Power</b> <span>100%</span>   |                          |                |              |                          |                |
| <b>Select SSID Profile</b>  |                          |                |              |                          |                |
| <b>Index</b>  | <b>Active</b>            | <b>Profile</b> | <b>Index</b> | <b>Active</b>            | <b>Profile</b> |
| 1   | <input type="checkbox"/> | VoIP_SSID      | 5            | <input type="checkbox"/> | SSID03         |
| 2   | <input type="checkbox"/> | Guest_SSID     | 6            | <input type="checkbox"/> | SSID03         |
| 3   | <input type="checkbox"/> | SSID03         | 7            | <input type="checkbox"/> | SSID03         |
| 4   | <input type="checkbox"/> | SSID03         | 8            | <input type="checkbox"/> | SSID03         |
| <input checked="" type="checkbox"/> <b>Enable Spanning Tree Protocol (STP)</b><br><input type="checkbox"/> <b>Enable Roaming</b><br><small>(The STP and Roaming are common settings. The changes are for both WLAN Interfaces.)</small> |                          |                |              |                          |                |
| <div> <span>Apply</span> <span>Reset</span> </div>  |                          |                |              |                          |                |

The following table describes the labels in this screen.

**Table 33** Wireless: Multiple BSS

| LABEL             | DESCRIPTION  |
|-------------------|--|
| WLAN Interface    | Select which WLAN adapter you want to configure.<br>It is recommended that you configure the first WLAN adapter for AP functions and use the second WLAN adapter for bridge functions.   |
| Operating Mode    | Select <b>MBSSID</b> in this field to display the screen as shown  |
| 802.11 Mode       | Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device.<br>Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device.<br>Select <b>802.11b+g</b> to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.<br>Select <b>802.11a</b> to allow only IEEE 802.11a compliant WLAN devices to associate with the ZyXEL Device. |
| Super Mode        | Select this to improve data throughput on the WLAN by enabling fast frame and packet bursting.   |
| Choose Channel ID | Set the operating frequency/channel depending on your particular region. To manually set the ZyXEL Device to use a channel, select a channel from the drop-down list box.<br>Click <b>MAINTENANCE</b> and then the <b>Channel Usage</b> tab to open the <b>Channel Usage</b> screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network. To have the ZyXEL Device automatically select a channel, click <b>Scan</b> instead.   |
| Scan              | Click this button to have the ZyXEL Device automatically select the wireless channel with the lowest interference.   |

**Table 33** Wireless: Multiple BSS

| LABEL                              | DESCRIPTION  |
|------------------------------------|--|
| Disable channel switching for DFS  | <p>This field is available when you select <b>802.11a</b> in the <b>802.11 Mode</b> field.</p> <p>DFS (dynamic frequency selection) allows an AP to detect other devices in the same channel. If there is another device using the same channel, the AP changes to a different channel, so that it can avoid interference with radar systems or other wireless networks.</p> <p>Select this option to disable DFS on the ZyXEL Device when <b>802.11 Mode</b> is set to <b>802.11a</b>.</p>  |
| RTS/CTS Threshold                  | <p>The threshold (number of bytes) for enabling RTS/CTS handshake. Data with a frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to its lowest value (256) turns on the RTS/CTS handshake. Enter a value between <b>256</b> and <b>2346</b>.</p> <p>This field is not available when <b>Super Mode</b> is selected.</p>   |
| Fragmentation Threshold            | <p>The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between <b>256</b> and <b>2346</b>.</p> <p>This field is not available when <b>Super Mode</b> is selected.</p>  |
| Output Power                       | <p>Set the output power of the ZyXEL Device in this field. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following <b>100%</b>, <b>50%</b>, <b>25%</b>, <b>12.5%</b> or <b>Minimum</b>. See the product specifications for more information on your ZyXEL Device's output power.</p> <p>This field is not available when you select <b>802.11a</b> in the <b>802.11 Mode</b> field.</p>   |
| Select SSID Profile                | <p>An SSID profile is the set of parameters relating to one of the ZyXEL Device's BSSs. The SSID (Service Set Identifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating with the access point (AP) must have the same SSID.</p> <p><b>Note:</b> If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or security settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.</p> |
| Index                              | This is the index number of the SSID profile.  |
| Active                             | Select the check box to activate an SSID profile.  |
| Profile                            | <p>Select the profile(s) of the SSIDs you want to use in your wireless network. You can have up to eight BSSs running on the ZyXEL Device simultaneously, one of which is always the pre-configured <b>VoIP_SSID</b> profile and another of which is always the pre-configured <b>Guest_SSID</b> profile.</p> <p>Configure SSID profiles in the <b>SSID</b> screen.</p>  |
| Enable Spanning Tree Control (STP) | <p>(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP - compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select the check box to activate STP on the ZyXEL Device.</p>   |

**Table 33** Wireless: Multiple BSS

| LABEL          | DESCRIPTION  |
|----------------|--|
| Enable Roaming | Roaming allows wireless stations to switch from one access point to another as they move from one coverage area to another. Select this checkbox to enable roaming on the ZyXEL Device if you have two or more ZyXEL Devices on the same subnet.<br><br>Note: All APs on the same subnet and the wireless stations must have the same SSID to allow roaming. |
| Apply          | Click <b>Apply</b> to save your changes.   |
| Reset          | Click <b>Reset</b> to begin configuring this screen afresh.  |

## 8.2 SSID

When the ZyXEL Device is set to Access Point, AP+Bridge or MBSSID mode, you need to choose the SSID profile(s) you want to use in your wireless network (see [Section 6.6 on page 92](#) for more information on operating modes).

Use the **WIRELESS > SSID** screen to see information about the SSID profiles on the ZyXEL Device, and use the **WIRELESS > SSID > Edit** screen to configure the SSID profiles.

### 8.2.1 The SSID Screen

Click **WIRELESS > SSID** to display the screen as shown.

**Figure 63** SSID

| Wireless | SSID  | Security     | RADIUS  | Layer-2 Isolation | MAC Filter |      |                   |            |
|----------|-------|--------------|---------|-------------------|------------|------|-------------------|------------|
|          | Index | Profile Name | SSID    | Security          | RADIUS     | QoS  | Layer-2 Isolation | MAC Filter |
|          | 1     | VoIP_SSID    | ZyXEL01 | security01        | radius01   | VoIP | Disable           | Disable    |
|          | 2     | Guest_SSID   | ZyXEL02 | security01        | radius01   | NONE | Isolation01       | Disable    |
|          | 3     | SSID03       | ZyXEL03 | security01        | radius01   | NONE | Disable           | Disable    |
|          | 4     | SSID04       | ZyXEL04 | security01        | radius01   | NONE | Disable           | Disable    |
|          | 5     | SSID05       | ZyXEL05 | security01        | radius01   | NONE | Disable           | Disable    |
|          | 6     | SSID06       | ZyXEL06 | security01        | radius01   | NONE | Disable           | Disable    |
|          | 7     | SSID07       | ZyXEL07 | security01        | radius01   | NONE | Disable           | Disable    |
|          | 8     | SSID08       | ZyXEL08 | security01        | radius01   | NONE | Disable           | Disable    |
|          | 9     | SSID09       | ZyXEL09 | security01        | radius01   | NONE | Disable           | Disable    |
|          | 10    | SSID10       | ZyXEL10 | security01        | radius01   | NONE | Disable           | Disable    |
|          | 11    | SSID11       | ZyXEL11 | security01        | radius01   | NONE | Disable           | Disable    |
|          | 12    | SSID12       | ZyXEL12 | security01        | radius01   | NONE | Disable           | Disable    |
|          | 13    | SSID13       | ZyXEL13 | security01        | radius01   | NONE | Disable           | Disable    |
|          | 14    | SSID14       | ZyXEL14 | security01        | radius01   | NONE | Disable           | Disable    |
|          | 15    | SSID15       | ZyXEL15 | security01        | radius01   | NONE | Disable           | Disable    |
|          | 16    | SSID16       | ZyXEL16 | security01        | radius01   | NONE | Disable           | Disable    |

Edit

The following table describes the labels in this screen.

**Table 34** SSID

| LABEL             | DESCRIPTION  |
|-------------------|--|
| Index             | This field displays the index number of each SSID profile.   |
| Name              | This field displays the identification name of each SSID profile on the ZyXEL Device.  |
| SSID              | This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility. |
| Security          | This field indicates which security profile is currently associated with each SSID profile. See <a href="#">Section 7.3 on page 103</a> for more information.  |
| RADIUS            | This field displays which RADIUS profile is currently associated with each SSID profile, if you have a RADIUS server configured.   |
| QoS               | This field displays the Quality of Service setting for this profile or <b>NONE</b> if QoS is not configured on a profile.  |
| Layer 2 Isolation | This field displays which layer 2 isolation profile is currently associated with each SSID profile, or <b>Disable</b> if Layer 2 Isolation is not configured on an SSID profile.                           |
| MAC Filter        | This field displays which MAC filter profile is currently associated with each SSID profile, or <b>Disable</b> if MAC filtering is not configured on an SSID profile.                                      |
| Edit              | Click the radio button next to the profile you want to configure and click <b>Edit</b> to go to the SSID configuration screen.   |

## 8.2.2 Configuring SSID

Each SSID profile references the settings configured in the following screens:

- **WIRELESS > Security** (one of the security profiles).
- **WIRELESS > RADIUS** (one of the RADIUS profiles).
- **WIRELESS > MAC Filter** (the MAC filter list, if activated in the SSID profile).
- **WIRELESS > Layer 2 Isolation** (the layer 2 isolation list, if activated in the SSID profile).
- Also, use the **VLAN** screen to set up wireless VLANs based on SSID.

Configure the fields in the above screens to use the settings in an SSID profile.

Select an SSID profile in the **WIRELESS > SSID** screen and click **Edit** to display the following screen.

**Figure 64** Configuring SSID

| Wireless                          | SSID       | Security | RADIUS | Layer-2 Isolation | MAC Filter |
|-----------------------------------|------------|----------|--------|-------------------|------------|
| Profile Name                      | SSID04     |          |        |                   |            |
| SSID                              | TA_PoM     |          |        |                   |            |
| Hide Name(SSID)                   | Disable    |          |        |                   |            |
| Security                          | security01 |          |        |                   |            |
| RADIUS                            | radius01   |          |        |                   |            |
| QoS                               | NONE       |          |        |                   |            |
| Layer-2 Isolation                 | Disable    |          |        |                   |            |
| Intra-BSS Traffic blocking        | Disable    |          |        |                   |            |
| MAC Filtering                     | Disable    |          |        |                   |            |
| <div>Apply</div> <div>Reset</div> |            |          |        |                   |            |

The following table describes the labels in this screen.

**Table 35** Configuring SSID

| LABEL            | DESCRIPTION   |
|------------------|---|
| Profile Name     | Enter a name identifying this profile.  |
| SSID             | When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.   |
| Hide Name (SSID) | Select <b>Disable</b> if you want the ZyXEL Device to broadcast this SSID (a wireless client scanning for an AP will find this SSID). Alternatively, select <b>Enable</b> to have the ZyXEL Device hide this SSID (a wireless client scanning for an AP will not find this SSID).   |
| Security         | Select a security profile to use with this SSID profile. See <a href="#">Section 7.3 on page 103</a> for more information.  |
| RADIUS           | Select a RADIUS profile from the drop-down list box, if you have a RADIUS server configured. If you do not need to use RADIUS authentication, ignore this field. See <a href="#">Section 7.5 on page 111</a> for more information.  |
| QoS              | <p>Select the Quality of Service priority for this BSS's traffic.</p> <ul style="list-style-type: none"> <li>In the pre-configured <b>VoIP_SSID</b> profile, the QoS setting is <b>VoIP</b>. This is not user-configurable. The <b>VoIP</b> setting is available only on the <b>VoIP_SSID</b> profile, and provides the highest level of QoS.</li> <li>If you select <b>WMM</b> from the <b>QoS</b> list, the priority of a data packet depends on the packet's IEEE 802.1q or DSCP header. See <a href="#">Section 6.3.1 on page 86</a> for more information on WMM and WMM priorities. If a packet has no WMM value assigned to it, it is assigned the default priority.</li> <li>If you select <b>ATC</b> from the <b>QoS</b> list, the ZyXEL Device automatically assigns priority based on packet size. See <a href="#">Section 6.3.2 on page 87</a> for more information on ATC.</li> <li>If you select <b>ATC+WMM</b> from the <b>QoS</b> list, the ZyXEL Device uses WMM on the wireless network and ATC on the wired network. See <a href="#">Section 6.3.3 on page 88</a> for more information on ATC+WMM.</li> <li>If you select <b>WMM_VOICE</b>, <b>WMM_VIDEO</b>, <b>WMM_BEST_EFFORT</b> or <b>WMM_BACKGROUND</b>, the ZyXEL Device applies that QoS setting to all of that SSID's traffic.</li> <li>If you select <b>NONE</b>, the ZyXEL Device applies no priority to traffic on this SSID.</li> </ul> <p>Note: When you configure an SSID profile's QoS settings, the ZyXEL Device applies the same QoS setting to all of the profile's traffic.</p> |

**Table 35** Configuring SSID

| LABEL                      | DESCRIPTION  |
|----------------------------|--|
| Layer-2 Isolation          | Select a layer 2 isolation profile from the drop-down list box. If you do not want to use layer 2 isolation on this profile, select <b>Disable</b> . See <a href="#">Section 9.1 on page 121</a> for more information. |
| Intra-BSS Traffic blocking | Select <b>Enable</b> from the drop-down list box to prevent wireless clients in this profile's BSS from communicating with one another.  |
| MAC Filtering              | Select a MAC filter profile from the drop-down list box. If you do not want to use MAC filtering on this profile, select <b>Disable</b> . See <a href="#">Section 9.4 on page 126</a> for more information.            |
| Apply                      | Click <b>Apply</b> to save your changes.   |
| Reset                      | Click <b>Reset</b> to begin configuring this screen afresh.  |

# Other Wireless Configuration

This chapter describes how to configure the **Layer-2 Isolation** and **MAC Filter** screens on your ZyXEL Device.

## 9.1 Layer-2 Isolation Introduction

Layer-2 isolation is used to prevent wireless clients associated with your ZyXEL Device from communicating with other wireless clients, APs, computers or routers in a network.

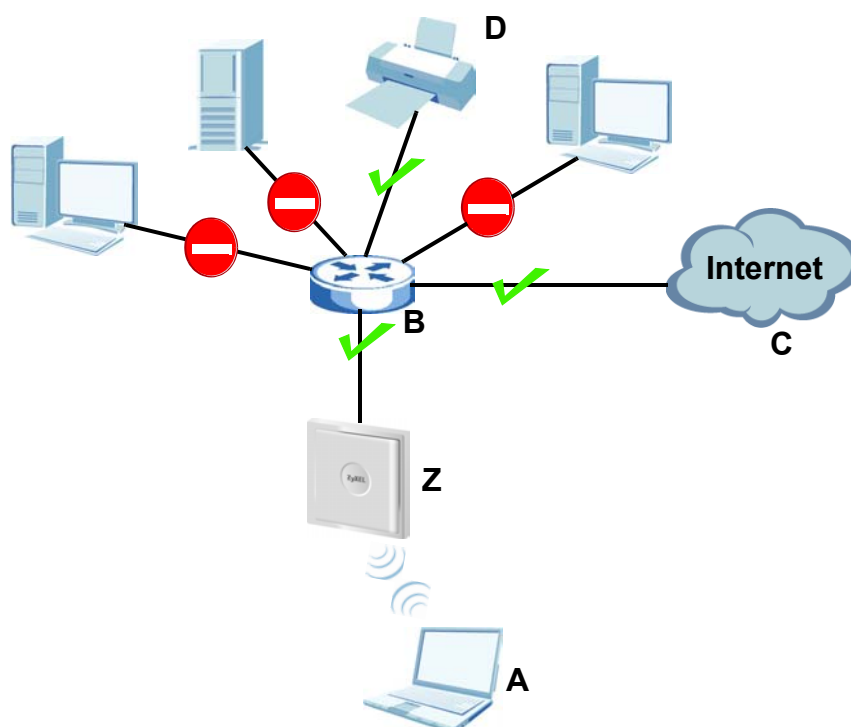
In the following example, layer-2 isolation is enabled on the ZyXEL Device (**Z**, in the figure) to allow a guest wireless client (**A**) to access the main network router (**B**). The router provides access to the Internet (**C**) and the network printer (**D**) while preventing the client from accessing other computers and servers on the network. The client can communicate with other wireless clients only if **Intra-BSS Traffic blocking** is disabled.



---

**Intra-BSS Traffic Blocking** is activated when you enable layer-2 isolation.

---

**Figure 65** Layer-2 Isolation Application

MAC addresses that are not listed in the **Allow devices with these MAC addresses** table are blocked from communicating with the ZyXEL Device's wireless clients except for broadcast packets. Layer-2 isolation does not check the traffic between wireless clients that are associated with the same AP. Intra-BSS Traffic allows wireless clients associated with the same AP to communicate with each other.

## 9.2 The Layer-2 Isolation Screen

Click **WIRELESS > Layer-2 Isolation**. The screen appears as shown next.

**Figure 66** WIRELESS > Layer 2 Isolation

| Wireless   | SSID  | Security      | RADIUS | Layer-2 Isolation | MAC Filter |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |
|--|-------|---------------|--------|-------------------|------------|--|-------|--------------|--|---|---------------|--|---|---------------|--|---|-----------|--|---|---------------|--|---|---------------|--|---|---------------|--|---|---------------|--|---|---------------|--|---|---------------|--|----|---------------|--|----|---------------|--|----|---------------|--|----|---------------|--|----|---------------|--|----|---------------|--|----|---------------|
| <table border="1"> <thead> <tr> <th></th> <th>Index</th> <th>Profile Name</th> </tr> </thead> <tbody> <tr><td></td><td>1</td><td>I2isolation01</td></tr> <tr><td></td><td>2</td><td>I2isolation02</td></tr> <tr><td></td><td>3</td><td>Guest_Iso</td></tr> <tr><td></td><td>4</td><td>I2isolation04</td></tr> <tr><td></td><td>5</td><td>I2isolation05</td></tr> <tr><td></td><td>6</td><td>I2isolation06</td></tr> <tr><td></td><td>7</td><td>I2isolation07</td></tr> <tr><td></td><td>8</td><td>I2isolation08</td></tr> <tr><td></td><td>9</td><td>I2isolation09</td></tr> <tr><td></td><td>10</td><td>I2isolation10</td></tr> <tr><td></td><td>11</td><td>I2isolation11</td></tr> <tr><td></td><td>12</td><td>I2isolation12</td></tr> <tr><td></td><td>13</td><td>I2isolation13</td></tr> <tr><td></td><td>14</td><td>I2isolation14</td></tr> <tr><td></td><td>15</td><td>I2isolation15</td></tr> <tr><td></td><td>16</td><td>I2isolation16</td></tr> </tbody> </table> |       |               |        |                   |            |  | Index | Profile Name |  | 1 | I2isolation01 |  | 2 | I2isolation02 |  | 3 | Guest_Iso |  | 4 | I2isolation04 |  | 5 | I2isolation05 |  | 6 | I2isolation06 |  | 7 | I2isolation07 |  | 8 | I2isolation08 |  | 9 | I2isolation09 |  | 10 | I2isolation10 |  | 11 | I2isolation11 |  | 12 | I2isolation12 |  | 13 | I2isolation13 |  | 14 | I2isolation14 |  | 15 | I2isolation15 |  | 16 | I2isolation16 |
|  | Index | Profile Name  |        |                   |            |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |
|  | 1     | I2isolation01 |        |                   |            |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |
|  | 2     | I2isolation02 |        |                   |            |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |
|  | 3     | Guest_Iso     |        |                   |            |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |
|  | 4     | I2isolation04 |        |                   |            |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |
|  | 5     | I2isolation05 |        |                   |            |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |
|  | 6     | I2isolation06 |        |                   |            |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |
|  | 7     | I2isolation07 |        |                   |            |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |
|  | 8     | I2isolation08 |        |                   |            |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |
|  | 9     | I2isolation09 |        |                   |            |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |
|  | 10    | I2isolation10 |        |                   |            |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |
|  | 11    | I2isolation11 |        |                   |            |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |
|  | 12    | I2isolation12 |        |                   |            |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |
|  | 13    | I2isolation13 |        |                   |            |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |
|  | 14    | I2isolation14 |        |                   |            |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |
|  | 15    | I2isolation15 |        |                   |            |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |
|  | 16    | I2isolation16 |        |                   |            |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |
| <input type="button" value="Edit"/>  |       |               |        |                   |            |  |       |              |  |   |               |  |   |               |  |   |           |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |   |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |  |    |               |

The following table describes the labels in this screen.

**Table 36** WIRELESS > Layer-2 Isolation

| LABEL        | DESCRIPTION   |
|--------------|---|
| Index        | This is the index number of the profile.  |
| Profile Name | This field displays the name given to a layer-2 isolation profile in the <b>Layer-2 Isolation Configuration</b> screen. |
| Edit         | Select an entry from the list and click <b>Edit</b> to configure settings for that profile.                             |

## 9.3 Configuring Layer-2 Isolation

To configure layer-2 isolation, click **WIRELESS > Layer-2 Isolation > Edit**. The screen appears as shown.



If layer-2 isolation is enabled, you need to know the MAC address of each wireless client, AP, computer or router that you want to allow to communicate with the ZyXEL Device's wireless clients.

**Figure 67** WIRELESS > Layer-2 Isolation Configuration Screen

| Wireless                               | SSID              | Security      | RADIUS | Layer-2 Isolation | MAC Filter  |
|--|-------------------|---------------|--------|-------------------|-------------|
| Layer 2 Isolation Configuration        |                   |               |        |                   |             |
| Profile Name                           |                   | l2isolation01 |        |                   |             |
| Allow devices with these MAC addresses |                   |               |        |                   |             |
| Index                                  | MAC Address       | Description   | Index  | MAC Address       | Description |
| 1                                      | 00:00:00:00:00:00 |               | 17     | 00:00:00:00:00:00 |             |
| 2                                      | 00:00:00:00:00:00 |               | 18     | 00:00:00:00:00:00 |             |
| 3                                      | 00:00:00:00:00:00 |               | 19     | 00:00:00:00:00:00 |             |
| 4                                      | 00:00:00:00:00:00 |               | 20     | 00:00:00:00:00:00 |             |
| 5                                      | 00:00:00:00:00:00 |               | 21     | 00:00:00:00:00:00 |             |
| 6                                      | 00:00:00:00:00:00 |               | 22     | 00:00:00:00:00:00 |             |
| 7                                      | 00:00:00:00:00:00 |               | 23     | 00:00:00:00:00:00 |             |
| 8                                      | 00:00:00:00:00:00 |               | 24     | 00:00:00:00:00:00 |             |
| 9                                      | 00:00:00:00:00:00 |               | 25     | 00:00:00:00:00:00 |             |
| 10                                     | 00:00:00:00:00:00 |               | 26     | 00:00:00:00:00:00 |             |
| 11                                     | 00:00:00:00:00:00 |               | 27     | 00:00:00:00:00:00 |             |
| 12                                     | 00:00:00:00:00:00 |               | 28     | 00:00:00:00:00:00 |             |
| 13                                     | 00:00:00:00:00:00 |               | 29     | 00:00:00:00:00:00 |             |
| 14                                     | 00:00:00:00:00:00 |               | 30     | 00:00:00:00:00:00 |             |
| 15                                     | 00:00:00:00:00:00 |               | 31     | 00:00:00:00:00:00 |             |
| 16                                     | 00:00:00:00:00:00 |               | 32     | 00:00:00:00:00:00 |             |

The following table describes the labels in this screen.

**Table 37** WIRELESS > Layer-2 Isolation Configuration

| LABEL                                  | DESCRIPTION  |
|--|--|
| Profile Name                           | Type a name to identify this layer-2 isolation profile.  |
| Allow devices with these MAC addresses | These are the MAC address of a wireless client, AP, computer or router. A wireless client associated with the ZyXEL Device can communicate with another wireless client, AP, computer or router only if the MAC addresses of those devices are listed in this table.                         |
| Index                                  | This is the index number of the MAC address.   |
| MAC Address                            | Type the MAC addresses of the wireless client, AP, computer or router that you want to allow the associated wireless clients to have access to in these address fields. Type the MAC address in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc). |
| Description                            | Type a name to identify this device.   |
| Apply                                  | Click <b>Apply</b> to save your changes.   |
| Reset                                  | Click <b>Reset</b> to begin configuring this screen afresh.  |

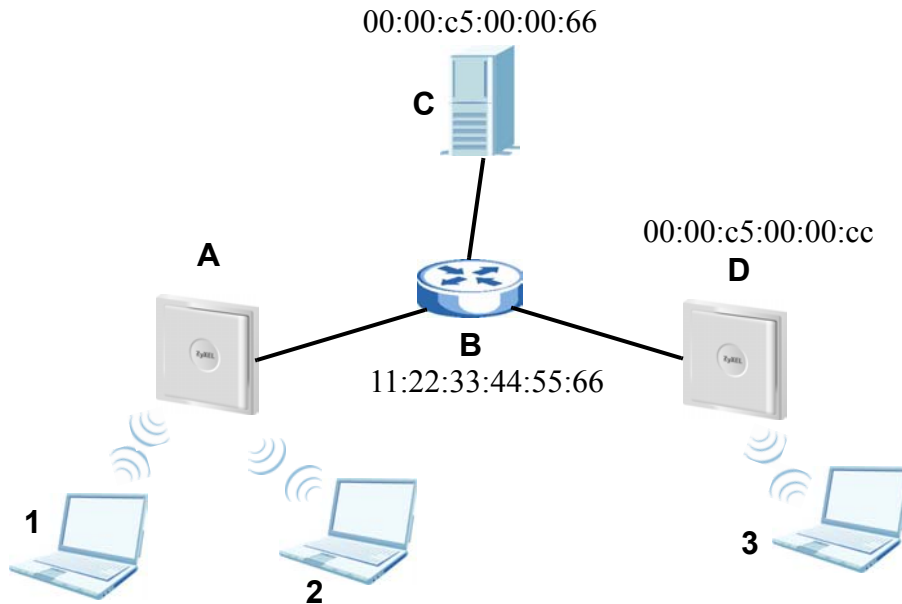
### 9.3.1 Layer-2 Isolation Examples

The following section shows you example layer-2 isolation configurations on the ZyXEL Device (A).



When configuring, remember to select the correct layer-2 isolation profile in the **WIRELESS > SSID > Edit** screen of the relevant SSID profile.

**Figure 68** Layer-2 Isolation Example Configuration



#### 9.3.1.1 Layer-2 Isolation Example 1

In the following example wireless clients **1** and **2** can communicate with network router **B** and file server **C**, but not access point **D** or wireless client **3**.

- Enter **B**'s MAC address in the **MAC Address** field, and enter "Network Router B" in **B**'s **Description** field. Enter **C**'s MAC address in the **MAC Address** field, and enter "File Server C" in **C**'s **Description** field.

**Figure 69** Layer-2 Isolation Example 1

| Wireless                               | SSID              | Security         | RADIUS | Layer-2 Isolation | MAC Filter  |
|--|-------------------|------------------|--------|-------------------|-------------|
| Layer-2 Isolation Configuration        |                   |                  |        |                   |             |
| Profile Name                           |                   | l2isolation01    |        |                   |             |
| Allow devices with these MAC addresses |                   |                  |        |                   |             |
| Index                                  | MAC Address       | Description      | Index  | MAC Address       | Description |
| 1                                      | 11:22:33:44:55:66 | Network Router B | 17     | 00:00:00:00:00:00 |             |
| 2                                      | 00:00:c5:00:00:66 | File Server C    | 18     | 00:00:00:00:00:00 |             |
| 3                                      | 00:00:00:00:00:00 |                  | 19     | 00:00:00:00:00:00 |             |

### 9.3.1.2 Layer-2 Isolation Example 2

In the following example wireless clients **1** and **2** can communicate with access point **D** and file server **C** but not wireless client **3**.

- Enter the router's, server's and access point **D**'s MAC addresses in the **MAC Address** fields. Enter "Network Router B" in **B**'s **Description** field, enter "File Server C" in **C**'s **Description** field, and enter "Access Point D" in **D**'s **Description** field.

**Figure 70** Layer-2 Isolation Example 2

| Wireless                               | SSID              | Security         | RADIUS | Layer-2 Isolation | MAC Filter  |
|--|-------------------|------------------|--------|-------------------|-------------|
| <b>Layer-2 Isolation Configuration</b> |                   |                  |        |                   |             |
| Profile Name                           |                   | l2isolation01    |        |                   |             |
| Allow devices with these MAC addresses |                   |                  |        |                   |             |
| Index                                  | MAC Address       | Description      | Index  | MAC Address       | Description |
| 1                                      | 11:22:33:44:55:66 | Network Router B | 17     | 00:00:00:00:00:00 |             |
| 2                                      | 00:00:c5:00:00:66 | File Server C    | 18     | 00:00:00:00:00:00 |             |
| 3                                      | 00:00:c5:00:00:cc | Access Point D   | 19     | 00:00:00:00:00:00 |             |
| 4                                      | 00:00:00:00:00:00 |                  | 20     | 00:00:00:00:00:00 |             |

## 9.4 The MAC Filter Screen

The MAC filter function allows you to configure the ZyXEL Device to give exclusive access to devices (**Allow Association**) or exclude devices from accessing the ZyXEL Device (**Deny Association**).

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of each device to configure MAC filtering on the ZyXEL Device.

The MAC filter profile is a user-configured list of MAC addresses. Each SSID profile can reference one MAC filter profile. The ZyXEL Device provides 16 MAC Filter profiles, each of which can hold up to 32 MAC addresses.

Click **WIRELESS > MAC Filter**. The screen displays as shown.

**Figure 71** WIRELESS > MAC Filter

| Wireless  | SSID  | Security     | RADIUS           | Layer-2 Isolation | MAC Filter |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
|---|-------|--------------|------------------|-------------------|------------|--|-------|--------------|---------------|--|---|-------------|------------------|--|---|-------------|------------------|--|---|-------------|------------------|--|---|-------------|------------------|--|---|-------------|------------------|--|---|-------------|------------------|--|---|-------------|------------------|--|---|-------------|------------------|--|---|-------------|------------------|--|----|-------------|------------------|--|----|-------------|------------------|--|----|-------------|------------------|--|----|-------------|------------------|--|----|-------------|------------------|--|----|-------------|------------------|--|----|-------------|------------------|
|   |       |              |                  |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
| <table><tr><th></th><th>Index</th><th>Profile Name</th><th>Filter Action</th></tr><tr><td></td><td>1</td><td>macfilter01</td><td>Deny Association</td></tr><tr><td></td><td>2</td><td>macfilter02</td><td>Deny Association</td></tr><tr><td></td><td>3</td><td>macfilter03</td><td>Deny Association</td></tr><tr><td></td><td>4</td><td>macfilter04</td><td>Deny Association</td></tr><tr><td></td><td>5</td><td>macfilter05</td><td>Deny Association</td></tr><tr><td></td><td>6</td><td>macfilter06</td><td>Deny Association</td></tr><tr><td></td><td>7</td><td>macfilter07</td><td>Deny Association</td></tr><tr><td></td><td>8</td><td>macfilter08</td><td>Deny Association</td></tr><tr><td></td><td>9</td><td>macfilter09</td><td>Deny Association</td></tr><tr><td></td><td>10</td><td>macfilter10</td><td>Deny Association</td></tr><tr><td></td><td>11</td><td>macfilter11</td><td>Deny Association</td></tr><tr><td></td><td>12</td><td>macfilter12</td><td>Deny Association</td></tr><tr><td></td><td>13</td><td>macfilter13</td><td>Deny Association</td></tr><tr><td></td><td>14</td><td>macfilter14</td><td>Deny Association</td></tr><tr><td></td><td>15</td><td>macfilter15</td><td>Deny Association</td></tr><tr><td></td><td>16</td><td>macfilter16</td><td>Deny Association</td></tr></table> |       |              |                  |                   |            |  | Index | Profile Name | Filter Action |  | 1 | macfilter01 | Deny Association |  | 2 | macfilter02 | Deny Association |  | 3 | macfilter03 | Deny Association |  | 4 | macfilter04 | Deny Association |  | 5 | macfilter05 | Deny Association |  | 6 | macfilter06 | Deny Association |  | 7 | macfilter07 | Deny Association |  | 8 | macfilter08 | Deny Association |  | 9 | macfilter09 | Deny Association |  | 10 | macfilter10 | Deny Association |  | 11 | macfilter11 | Deny Association |  | 12 | macfilter12 | Deny Association |  | 13 | macfilter13 | Deny Association |  | 14 | macfilter14 | Deny Association |  | 15 | macfilter15 | Deny Association |  | 16 | macfilter16 | Deny Association |
|   | Index | Profile Name | Filter Action    |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
|   | 1     | macfilter01  | Deny Association |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
|   | 2     | macfilter02  | Deny Association |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
|   | 3     | macfilter03  | Deny Association |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
|   | 4     | macfilter04  | Deny Association |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
|   | 5     | macfilter05  | Deny Association |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
|   | 6     | macfilter06  | Deny Association |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
|   | 7     | macfilter07  | Deny Association |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
|   | 8     | macfilter08  | Deny Association |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
|   | 9     | macfilter09  | Deny Association |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
|   | 10    | macfilter10  | Deny Association |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
|   | 11    | macfilter11  | Deny Association |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
|   | 12    | macfilter12  | Deny Association |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
|   | 13    | macfilter13  | Deny Association |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
|   | 14    | macfilter14  | Deny Association |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
|   | 15    | macfilter15  | Deny Association |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
|   | 16    | macfilter16  | Deny Association |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |
| <div>Edit</div>   |       |              |                  |                   |            |  |       |              |               |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |   |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |  |    |             |                  |

The following table describes the labels in this screen.

**Table 38** WIRELESS > MAC Filter

| LABEL         | DESCRIPTION   |
|---------------|---|
| Index         | This is the index number of the profile.  |
| Profile Name  | This field displays the name given to a MAC filter profile in the <b>MAC Filter Configuration</b> screen. |
| Filter Action | This is the filter action for the list of MAC addresses in the profile.                                   |
| Edit          | Select an entry from the list and click <b>Edit</b> to configure settings for that profile.               |

### 9.4.1 Configuring MAC Filtering

To change your ZyXEL Device's MAC filter settings, click **WIRELESS > MAC Filter > Edit**. The screen appears as shown.

**Figure 72** MAC Address Filter

| Wireless                  | SSID              | Security           | RADIUS | Layer-2 Isolation | MAC Filter  |
|---------------------------|-------------------|--------------------|--------|-------------------|-------------|
| <b>MAC Address Filter</b> |                   |                    |        |                   |             |
| <b>Profile Name</b>       |                   | macfilter01        |        |                   |             |
| <b>Filter Action</b>      |                   | Deny Association ▼ |        |                   |             |
| Index                     | MAC Address       | Description        | Index  | MAC Address       | Description |
| 1                         | 00:00:00:00:00:00 |                    | 17     | 00:00:00:00:00:00 |             |
| 2                         | 00:00:00:00:00:00 |                    | 18     | 00:00:00:00:00:00 |             |
| 3                         | 00:00:00:00:00:00 |                    | 19     | 00:00:00:00:00:00 |             |
| 4                         | 00:00:00:00:00:00 |                    | 20     | 00:00:00:00:00:00 |             |
| 5                         | 00:00:00:00:00:00 |                    | 21     | 00:00:00:00:00:00 |             |
| 6                         | 00:00:00:00:00:00 |                    | 22     | 00:00:00:00:00:00 |             |
| 7                         | 00:00:00:00:00:00 |                    | 23     | 00:00:00:00:00:00 |             |
| 8                         | 00:00:00:00:00:00 |                    | 24     | 00:00:00:00:00:00 |             |
| 9                         | 00:00:00:00:00:00 |                    | 25     | 00:00:00:00:00:00 |             |
| 10                        | 00:00:00:00:00:00 |                    | 26     | 00:00:00:00:00:00 |             |
| 11                        | 00:00:00:00:00:00 |                    | 27     | 00:00:00:00:00:00 |             |
| 12                        | 00:00:00:00:00:00 |                    | 28     | 00:00:00:00:00:00 |             |
| 13                        | 00:00:00:00:00:00 |                    | 29     | 00:00:00:00:00:00 |             |
| 14                        | 00:00:00:00:00:00 |                    | 30     | 00:00:00:00:00:00 |             |
| 15                        | 00:00:00:00:00:00 |                    | 31     | 00:00:00:00:00:00 |             |
| 16                        | 00:00:00:00:00:00 |                    | 32     | 00:00:00:00:00:00 |             |

The following table describes the labels in this screen.

**Table 39** MAC Address Filter

| LABEL         | DESCRIPTION  |
|---------------|--|
| Profile Name  | Type a name to identify this profile.  |
| Filter Action | Define the filter action for the list of MAC addresses in the MAC address filter table.<br>Select <b>Deny Association</b> to block access to the router. MAC addresses not listed will be allowed to access the router.<br>Select <b>Allow Association</b> to permit access to the router. MAC addresses not listed will be denied access to the router. |
| Index         | This is the index number of the MAC address.   |
| MAC Address   | Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station to be allowed or denied access to the ZyXEL Device.  |
| Description   | Type a name to identify this wireless station.   |
| Apply         | Click <b>Apply</b> to save your changes.   |
| Reset         | Click <b>Reset</b> to begin configuring this screen afresh.  |



---

To activate MAC filtering on an SSID profile, select the correct filter from the **Enable MAC Filtering** drop-down list box in the **WIRELESS > SSID > Edit** screen and click **Apply**.

---

## 9.5 Configuring Roaming

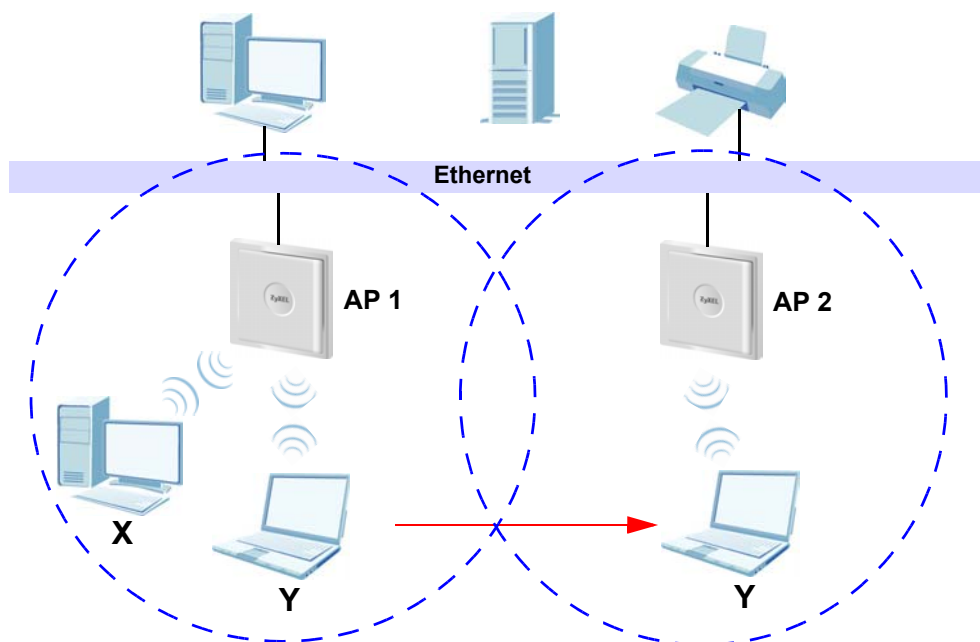
A wireless station is a device with an IEEE 802.11a/b/g compliant wireless interface. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access point's coverage area.

In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is known as roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending on the signal strength, network utilization or other factors.

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the other access points on the LAN about the change. An example is shown in [Figure 73 on page 130](#).

With roaming, a wireless LAN mobile user enjoys a continuous connection to the wired network through an access point while moving around the wireless LAN.

Enable roaming to exchange the latest bridge information of all wireless stations between APs when a wireless station moves between coverage areas. Wireless stations can still associate with other APs even if you disable roaming. Enabling roaming ensures correct traffic forwarding (bridge tables are updated) and maximum AP efficiency. The AP deletes records of wireless stations that associate with other APs (Non-ZyXEL APs may not be able to perform this). 802.1x authentication information is not exchanged (at the time of writing).

**Figure 73** Roaming Example

The steps below describe the roaming process.

- 1 Wireless station **Y** moves from the coverage area of access point **AP 1** to that of access point **AP 2**.
- 2 Wireless station **Y** scans and detects the signal of access point **AP 2**.
- 3 Wireless station **Y** sends an association request to access point **AP 2**.
- 4 Access point **AP 2** acknowledges the presence of wireless station **Y** and relays this information to access point **AP 1** through the wired LAN.
- 5 Access point **AP 1** updates the new position of wireless station **Y**.

### 9.5.1 Requirements for Roaming

The following requirements must be met in order for wireless stations to roam between the coverage areas.

- 1 All the access points must be on the same subnet and configured with the same ESSID.
- 2 If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.
- 3 The adjacent access points should use different radio channels when their coverage areas overlap.
- 4 All access points must use the same port number to relay roaming information.
- 5 The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

To enable roaming on your ZyXEL Device, click **WIRELESS > Wireless**. The screen appears as shown.

**Figure 74** Roaming

| Wireless   | SSID | Security | RADIUS | Layer-2 Isolation | MAC Filter |
|--|------|----------|--------|-------------------|------------|
| <b>WLAN Interface</b> <span>WLAN1</span>   |      |          |        |                   |            |
| <b>Operating Mode</b> <span>Access Point</span>  |      |          |        |                   |            |
| <b>802.11 Mode</b> <span>802.11b+g</span>  |      |          |        |                   |            |
| <input checked="" type="checkbox"/> <b>Super Mode</b>  |      |          |        |                   |            |
| <b>Choose Channel ID</b> <span>Channel-06 2437MHz</span> or <span>Scan</span>  |      |          |        |                   |            |
| <b>RTS/CTS Threshold</b> <span>2346</span> <small>(256 ~ 2346)</small>   |      |          |        |                   |            |
| <b>Fragmentation Threshold</b> <span>2346</span> <small>(256 ~ 2346) (Fragmentation threshold shall be an even number)</small> |      |          |        |                   |            |
| <b>Output Power</b> <span>100%</span>  |      |          |        |                   |            |
| <b>SSID Profile</b> <span>SSID03</span>  |      |          |        |                   |            |
| <input checked="" type="checkbox"/> <b>Enable Spanning Tree Protocol (STP)</b>   |      |          |        |                   |            |
| <input checked="" type="checkbox"/> <b>Enable Roaming</b>  |      |          |        |                   |            |
| <small>(The STP and Roaming are common settings. The changes are for both WLAN Interfaces.)</small>                            |      |          |        |                   |            |
| <div><span>Apply</span><span>Reset</span></div>  |      |          |        |                   |            |

Select the **Enable Roaming** check box and click **Apply**.



# IP Screen

This chapter discusses how to configure IP settings on the ZyXEL Device.

## 10.1 Factory Ethernet Defaults

The Ethernet parameters of the ZyXEL Device are preset in the factory with the following values:

- 1 IP address of 192.168.1.2
- 2 Subnet mask of 255.255.255.0 (24 bits)

These parameters should work for the majority of installations.

## 10.2 TCP/IP Parameters

### 10.2.1 WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet (only between your two branch offices, for instance) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

**Table 40** Private IP Address Ranges

|             |   |                 |
|-------------|---|-----------------|
| 10.0.0.0    | - | 10.255.255.255  |
| 172.16.0.0  | - | 172.31.255.255  |
| 192.168.0.0 | - | 192.168.255.255 |

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.



Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

## 10.3 Configuring IP Settings

Click **IP** to display the screen shown next.

**Figure 75** IP Setup

The following table describes the labels in this screen.

**Table 41** IP Setup

| LABEL                       | DESCRIPTION  |
|-----------------------------|--|
| IP Address Assignment       |  |
| Get automatically from DHCP | Select this option if your ZyXEL Device is using a dynamically assigned IP address from a DHCP server each time.<br><br>Note: You must know the IP address assigned to the ZyXEL Device (by the DHCP server) to access the ZyXEL Device again.   |
| Use fixed IP address        | Select this option if your ZyXEL Device is using a static IP address. When you select this option, fill in the fields below.   |
| IP Address                  | Enter the IP address of your ZyXEL Device in dotted decimal notation.<br><br>Note: If you change the ZyXEL Device's IP address, you must use the new IP address if you want to access the web configurator again.  |
| IP Subnet Mask              | Type the subnet mask.  |
| Gateway IP Address          | Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyXEL Device that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyXEL Device; over the WAN, the gateway must be the IP address of one of the remote nodes. |

**Table 41** IP Setup

| LABEL | DESCRIPTION   |
|-------|---|
| Apply | Click <b>Apply</b> to save your changes.                    |
| Reset | Click <b>Reset</b> to begin configuring this screen afresh. |



# Rogue AP

This chapter discusses rogue wireless access points (APs) and how to configure the ZyXEL Device's rogue AP detection feature.

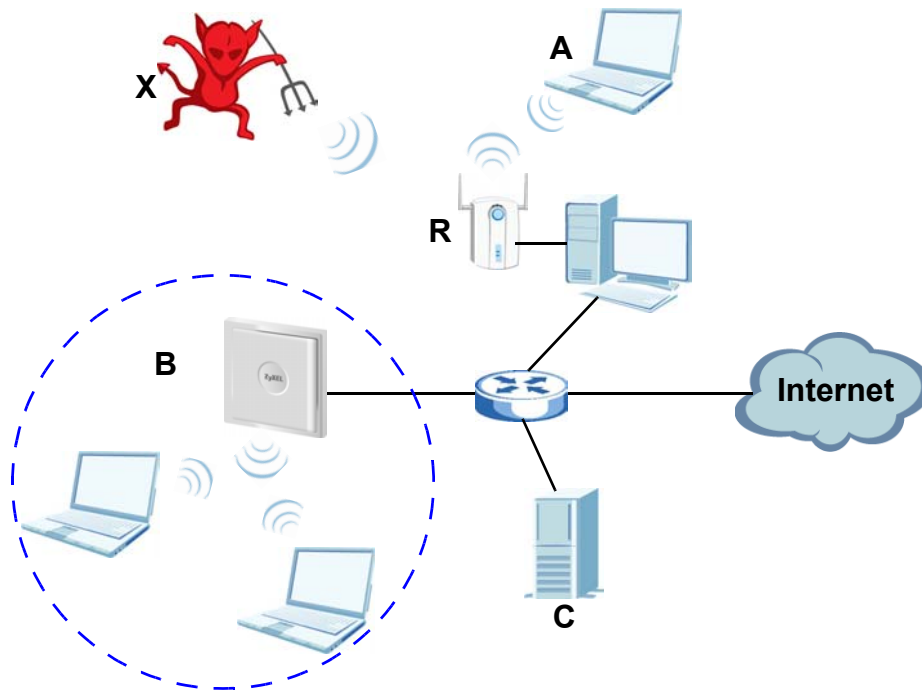
## 11.1 Rogue AP Introduction

A rogue AP is a wireless access point operating in a network's coverage area that is not a sanctioned part of that network. Rogue APs are not under the control of the network's administrators, and can open up holes in a network's security. Attackers can take advantage of a rogue AP's weaker (or non-existent) security to gain access to the network, or set up their own rogue APs in order to capture information from wireless clients. If a scan reveals a rogue AP, you can use commercially-available software to physically locate it.

Note that it is not necessary for a network to have a legitimate wireless LAN component for rogue APs to open the network to an attacker. In this case, any AP detected can be classified as rogue.

## 11.2 Rogue AP Examples

In the following example, a corporate network's security is compromised by a rogue AP (**R**) set up by an employee at his workstation in order to allow him to connect his notebook computer wirelessly (**A**). The company's legitimate wireless network (the dashed ellipse **B**) is well-secured, but the rogue AP uses inferior security that is easily broken by an attacker (**X**) running readily available encryption-cracking software. In this example, the attacker now has access to the company network, including sensitive data stored on the file server (**C**).

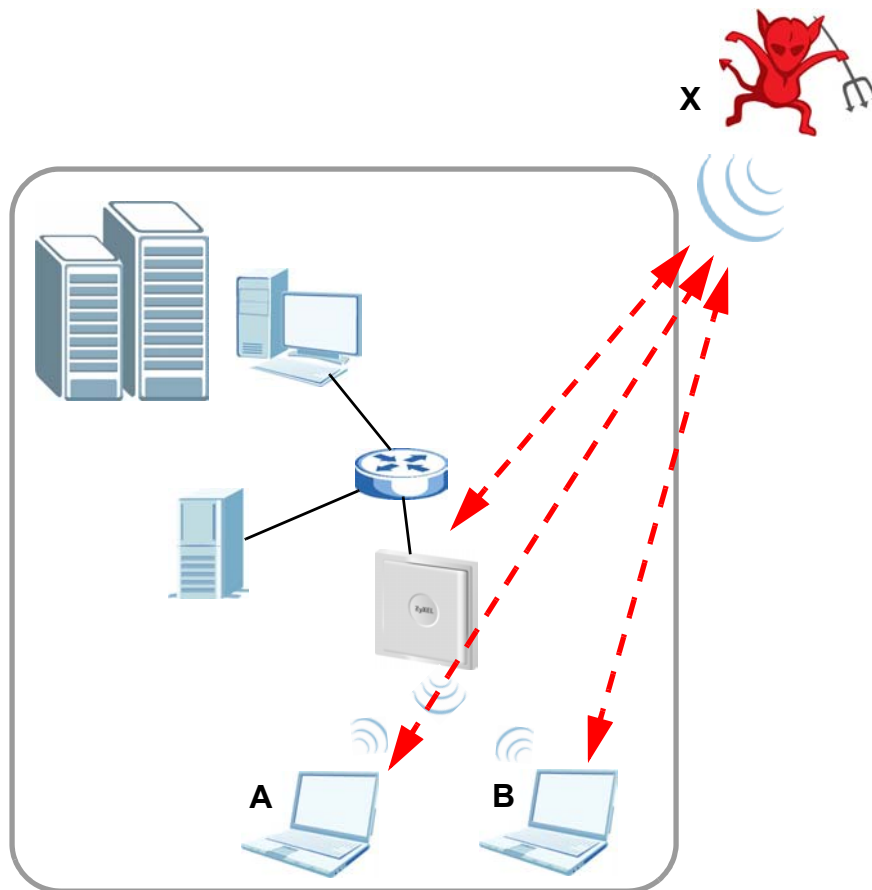
**Figure 76** Rogue AP: Example

### 11.2.1 “Honeypot” Attack

Rogue APs need not be connected to the legitimate network to pose a severe security threat. In the following example, an attacker (X) is stationed in a vehicle outside a company building, using a rogue access point equipped with a powerful antenna. By mimicking a legitimate (company network) AP, the attacker tries to capture usernames, passwords, and other sensitive information from unsuspecting clients (A and B) who attempt to connect. This is known as a “honeypot” attack.

If a rogue AP in this scenario has sufficient power and is broadcasting the correct SSID (Service Set Identifier) clients have no way of knowing that they are not associating with a legitimate company AP. The attacker can forward network traffic from associated clients to a legitimate AP, creating the impression of normal service. This is a variety of “man-in-the-middle” attack.

This scenario can also be part of a wireless denial of service (DoS) attack, in which associated wireless clients are deprived of network access. Other opportunities for the attacker include the introduction of malware (malicious software) into the network.

**Figure 77** “Honeypot” Attack

## 11.3 Configuring Rogue AP Detection

You can configure the ZyXEL Device to detect rogue IEEE 802.11a (5 GHz) and IEEE 802.11b/g (2.4 GHz) APs.

If you have more than one AP in your wireless network, you must also configure the list of “friendly” APs. Friendly APs are the other wireless access points in your network, as well as any others that you know are not a threat (those from neighboring networks, for example). It is recommended that you export (save) your list of friendly APs often, especially if you have a network with a large number of access points.

You can choose to scan for rogue APs manually, or to have the ZyXEL Device scan automatically at pre-defined intervals.

You can also set the ZyXEL Device to email you immediately when a rogue AP is detected (see [Chapter 15 on page 187](#) for information on how to set up email logs).

### 11.3.1 Rogue AP: Configuration

Click **ROGUE AP > Configuration**. The following screen appears.

**Figure 78** ROGUE AP > Configuration

The following table describes the labels in this screen.

**Table 42** ROGUE AP > Configuration

| LABEL                     | DESCRIPTION  |
|---------------------------|--|
| Rogue AP Period Detection | Select <b>Enable</b> to turn rogue AP detection on. You must also enter a time value in the <b>Period</b> field.<br>Select <b>Disable</b> to turn rogue AP detection off.                        |
| Period (minutes)          | Enter the period you want the ZyXEL Device to wait between scanning for rogue APs (between 10 and 60 minutes). You must also select <b>Enable</b> in the <b>Rogue AP Period Detection</b> field. |
| Expiration Time (minutes) | Specify how long (between 30 and 180 minutes) an AP's entry can remain in the <b>Rogue AP List</b> before the ZyXEL Device removes it from the list if the AP is no longer active.               |
| Friendly AP List          |  |
| Export                    | Click this button to save the current list of friendly APs' MAC addresses and descriptions (as displayed in the <b>ROGUE AP &gt; Friendly AP</b> screen) to your computer.                       |
| File Path                 | Enter the location of a previously-saved friendly AP list to upload to the ZyXEL Device. Alternatively, click the <b>Browse</b> button to locate a list.   |
| Browse                    | Click this button to locate a previously-saved list of friendly APs to upload to the ZyXEL Device.   |
| Import                    | Click this button to upload the previously-saved list of friendly APs displayed in the <b>File Path</b> field to the ZyXEL Device.   |
| Apply                     | Click <b>Apply</b> to save your settings.  |
| Reset                     | Click <b>Reset</b> to return all fields in this screen to their previously-saved values.   |

### 11.3.2 Rogue AP: Friendly AP

The friendly AP list displays details of all the access points in your area that you know are not a threat. If you have more than one AP in your network, you need to configure this list to include your other APs. If your wireless network overlaps with that of a neighbor (for example) you should also add these APs to the list, as they do not compromise your own network's security. If you do not add them to the friendly AP list, these access points will appear in the **Rogue AP** list each time the ZyXEL Device scans.

**Figure 79** ROGUE AP > Friendly AP

| Configuration   Friendly AP   Rogue AP |                   |                      |         |          |           |                                    |  |
|--|-------------------|----------------------|---------|----------|-----------|------------------------------------|--|
| Add Friendly AP                        |                   |                      |         |          |           |                                    |  |
| MAC Address                            |                   | Description          |         |          |           |                                    |  |
| <input type="text"/>                   |                   | <input type="text"/> |         |          |           | <input type="button" value="Add"/> |  |
| Friendly AP List                       |                   |                      |         |          |           |                                    |  |
| #                                      | MAC Address       | SSID                 | Channel | Security | Last Seen | Description                        |  |
| 1                                      | 06:19:cb:51:ef:cf | ZyXEL04              | 6       | WPA2-MIX | 8:58:26   | N/A                                |  |

The following table describes the labels in this screen.

**Table 43** ROGUE AP > Friendly AP

| LABEL            | DESCRIPTION   |
|------------------|---|
| Add Friendly AP  | Use this section to manually add a wireless access point to the list. You must know the device's MAC address.   |
| MAC Address      | Enter the MAC address of the AP you wish to add to the list.  |
| Description      | Enter a short, explanatory description identifying the AP with a maximum of 32 alphanumeric characters. Spaces, underscores ( _ ) and dashes ( - ) are allowed. |
| Add              | Click this button to include the AP in the list.  |
| Friendly AP List | This is the list of safe wireless access points you have already configured.  |
| #                | This is the index number of the AP's entry in the list.   |
| MAC Address      | This field displays the Media Access Control (MAC) address of the AP. All wireless devices have a MAC address that uniquely identifies them.                    |
| SSID             | This field displays the Service Set IDentifier (also known as the network name) of the AP.  |
| Channel          | This field displays the wireless channel the AP is currently using.   |
| Security         | This field displays the type of wireless encryption the AP is currently using.  |
| Last Seen        | This field displays the last time the ZyXEL Device scanned for the AP.  |
| Description      | This is the description you entered when adding the AP to the list.   |
| Delete           | Click this button to remove an AP's entry from the list.  |

### 11.3.3 Rogue AP List

This list displays details of all IEEE 802.11a/b/g wireless access points within the ZyXEL Device's coverage area, except for the ZyXEL Device itself and the access points included in the friendly AP list (see [Section 11.3.2 on page 140](#)).

You can set how often you want the ZyXEL Device to scan for rogue APs in the **ROGUE AP > Configuration** screen (see [Section 11.3.1 on page 139](#)).

Click **ROGUE AP > Rogue AP**. The following screen displays.

**Figure 80** ROGUE AP > Rogue AP

| # | Active                   | MAC Address       | SSID                 | Channel | Security | Last Seen | Description |
|---|--------------------------|-------------------|----------------------|---------|----------|-----------|-------------|
| 1 | <input type="checkbox"/> | 00:13:49:AF:A9:0F | USG200_FieldTrial_01 | 6       | None     | 17:04:16  |             |
| 2 | <input type="checkbox"/> | 06:13:49:AF:A9:0F | USG200_FieldTrial_02 | 6       | WPA-PSK  | 17:04:16  |             |
| 3 | <input type="checkbox"/> | 00:13:49:00:00:01 | ZyXEL03              | 6       | None     | 17:04:16  |             |
| 4 | <input type="checkbox"/> | 00:19:CB:51:EF:CF | pntest               | 6       | WPA2-MIX | 17:04:16  |             |

The following table describes the labels in this screen.

**Table 44** ROGUE AP > Rogue AP

| LABEL                   | DESCRIPTION  |
|-------------------------|--|
| Rogue AP List           | This displays details of access points in the ZyXEL Device's coverage area that are not listed in the friendly AP list (see <a href="#">Section 11.3.2 on page 140</a> )   |
| Refresh                 | Click this button to have the ZyXEL Device scan for rogue APs.   |
| #                       | This is the index number of the AP's entry in the list.  |
| Active                  | Use this check box to select the APs you want to move to the friendly AP list (see <a href="#">Section 11.3.2 on page 140</a> ).   |
| MAC Address             | This field displays the Media Access Control (MAC) address of the AP. All wireless devices have a MAC address that uniquely identifies them.   |
| SSID                    | This field displays the Service Set IDentifier (also known as the network name) of the AP.   |
| Channel                 | This field displays the wireless channel the AP is currently using.  |
| Security                | This field displays the type of wireless encryption the AP is currently using.   |
| Last Seen               | This field displays the last time the ZyXEL Device scanned for the AP.   |
| Description             | If you want to move the AP's entry to the friendly AP list, enter a short, explanatory description identifying the AP before you click <b>Add to Friendly AP List</b> . A maximum of 32 alphanumeric characters are allowed in this field. Spaces, underscores (_) and dashes (-) are allowed.   |
| Add to Friendly AP List | If you know that the AP described in an entry is not a threat, select the <b>Active</b> check box, enter a short description in the <b>Description</b> field and click this button to add the entry to the friendly AP list (see <a href="#">Section 11.3.2 on page 140</a> ). When the ZyXEL Device next scans for rogue APs, the selected AP does not appear in the rogue AP list. |
| Reset                   | Click <b>Reset</b> to return all fields in this screen to their default values.  |

# Remote Management Screens

This chapter provides information on the Remote Management screens.

## 12.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyXEL Device interface (if any) from which computers.

You may manage your ZyXEL Device from a remote location via:

**Table 45** Remote Management Overview

- |            |                      |
|------------|----------------------|
| • WLAN     | • ALL (LAN and WLAN) |
| • LAN only | • Neither (Disable). |

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

You may only have one remote management session running at a time. The ZyXEL Device automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

- 1 Console port
- 2 SSH
- 3 Telnet
- 4 HTTPS and HTTP

### 12.1.1 Remote Management Limitations

Remote management over LAN or WLAN will not work when:

- 1 You have disabled that service in one of the remote management screens.
- 2 The IP address in the **Secured Client IP Address** field does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.
- 3 There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

### 12.1.2 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The ZyXEL Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **System** screen

## 12.2 SSH

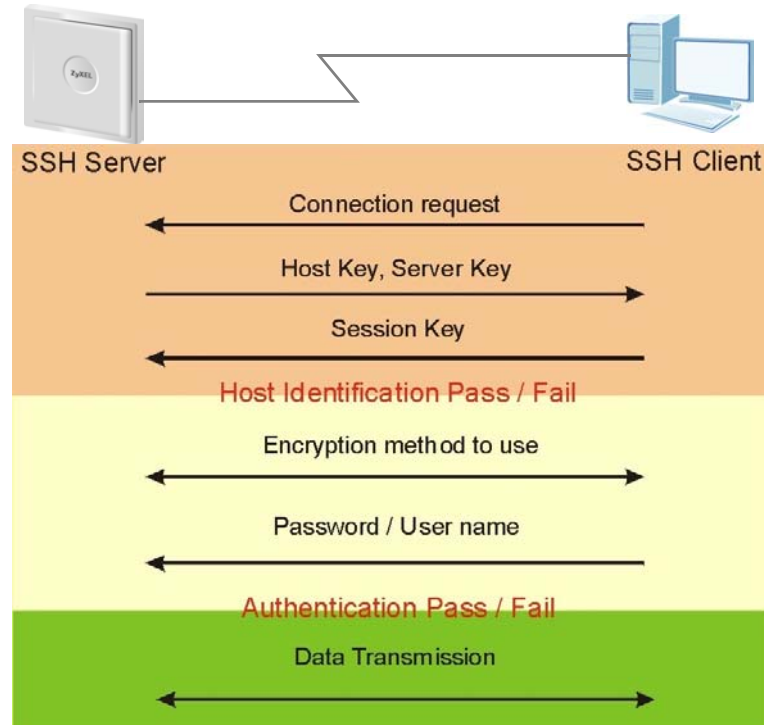
You can use SSH (Secure SHell) to securely access the ZyXEL Device's SMT or command line interface. Specify which interfaces allow SSH access and from which IP address the access can come.

Unlike Telnet or FTP, which transmit data in plaintext (clear or unencrypted text), SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

## 12.3 How SSH Works

The following table summarizes how a secure connection is established between two remote hosts.

**Figure 81** How SSH Works



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

**2 Encryption Method**

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

**3 Authentication and Data Transmission**

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

## 12.4 SSH Implementation on the ZyXEL Device

Your ZyXEL Device supports SSH version 1.0 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the ZyXEL Device for remote SMT management and file transfer on port 22. Only one SSH connection is allowed at a time.

### 12.4.1 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the ZyXEL Device over SSH.

## 12.5 Configuring Telnet

You can use Telnet to access the ZyXEL Device's SMT or command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

Click the **REMOTE MGNT > TELNET**. The following screen displays.



---

It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

---

**Figure 82** Remote Management: Telnet

The screenshot shows the 'Remote Management: Telnet' configuration interface. At the top, there are four tabs: TELNET, FTP, WWW, and SNMP. The 'TELNET' tab is selected. Below the tabs, there are two main sections: 'TELNET' and 'SSH'. Each section contains three configuration fields: 'Server Port', 'Server Access', and 'Secured Client IP Address'. In the 'TELNET' section, 'Server Port' is set to 23, 'Server Access' is set to 'WLAN & LAN', and 'Secured Client IP Address' has radio buttons for 'All' (selected) and 'Selected' (unselected), with a text box containing '0.0.0.0'. In the 'SSH' section, 'Server Certificate' is set to 'auto\_generated\_self\_signed\_cert' with a link '(See My Certificates)', 'Server Port' is set to 22, 'Server Access' is set to 'WLAN & LAN', and 'Secured Client IP Address' has radio buttons for 'All' (selected) and 'Selected' (unselected), with a text box containing '0.0.0.0'. At the bottom of the screen, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

**Table 46** Remote Management: Telnet

| LABEL                     | DESCRIPTION   |
|---------------------------|---|
| TELNET                    |   |
| Server Port               | You can change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.  |
| Server Access             | Select the interface(s) through which a computer may access the ZyXEL Device using Telnet.  |
| Secured Client IP Address | A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service.<br>Select <b>All</b> to allow any computer to access the ZyXEL Device using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service. |
| SSH                       |   |
| Server Certificate        | Select the certificate whose corresponding private key is to be used to identify the ZyXEL Device for SSH connections. You must have certificates already configured in the <b>CERTIFICATES &gt; My Certificates</b> screen.  |
| Server Port               | You can change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.  |
| Server Access             | Select the interface(s) through which a computer may access the ZyXEL Device using SSH.   |
| Secured Client IP Address | A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service.<br>Select <b>All</b> to allow any computer to access the ZyXEL Device using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service. |
| Apply                     | Click <b>Apply</b> to save your customized settings and exit this screen.   |
| Reset                     | Click <b>Reset</b> to begin configuring this screen afresh.   |

## 12.6 Configuring FTP

You can use FTP (File Transfer Protocol) to upload and download the ZyXEL Device's firmware and configuration files, please see the User's Guide chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

To change your ZyXEL Device's FTP settings, click **REMOTE MGNT > FTP**. The screen appears as shown. Use this screen to specify which interfaces allow FTP access and from which IP address the access can come.



It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

**Figure 83** Remote Management: FTP

The screenshot shows the 'Remote Management: FTP' configuration interface. It features four tabs: TELNET, FTP (which is the active tab), WWW, and SNMP. Below the tabs, the 'FTP' section is highlighted. There are three main configuration fields: 'Server Port' with a text box containing '21', 'Server Access' with a dropdown menu showing 'WLAN & LAN', and 'Secured Client IP Address' with radio buttons for 'All' (selected) and 'Selected', followed by a text box containing '0.0.0.0'. At the bottom of the form are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

**Table 47** Remote Management: FTP

| LABEL                     | DESCRIPTION  |
|---------------------------|--|
| Server Port               | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.   |
| Server Access             | Select the interface(s) through which a computer may access the ZyXEL Device using this service.   |
| Secured Client IP Address | A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service.<br>Select <b>All</b> to allow any computer to access the ZyXEL Device using this service.<br>Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service. |
| Apply                     | Click <b>Apply</b> to save your customized settings and exit this screen.  |
| Reset                     | Click <b>Reset</b> to begin configuring this screen afresh.  |

## 12.7 WWW (HTTP and HTTPS)

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

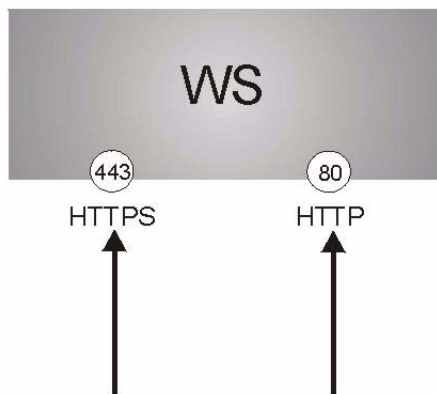
It relies upon certificates, public keys, and private keys (see [Chapter 15 on page 349](#) for more information).

HTTPS on the ZyXEL Device is used so that you may securely access the ZyXEL Device using the web configurator. The SSL protocol specifies that the SSL server (the ZyXEL Device) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyXEL Device), whereas the SSL client only should authenticate itself when the SSL server requires it to do so (select **Authenticate Client Certificates** in the **REMOTE MGMT > WWW** screen). **Authenticate Client Certificates** is optional and if selected means the SSL-client must send the ZyXEL Device a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the ZyXEL Device.

Please refer to the following figure.

- 1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the ZyXEL Device's WS (web server).
- 2 HTTP connection requests from a web browser go to port 80 (by default) on the ZyXEL Device's WS (web server).

**Figure 84** HTTPS Implementation



If you disable the **HTTP** service in the **REMOTE MGMT > WWW** screen, then the ZyXEL Device blocks all HTTP connection attempts.

## 12.8 Configuring WWW

To change your ZyXEL Device's World Wide Web settings, click **REMOTE MGNT > WWW**.

**Figure 85** Remote Management: WWW

The screenshot shows the 'Remote Management: WWW' configuration page. It has a header 'WWW' and a sub-header 'HTTPS'. Under 'WWW', there are three settings: 'Server Port' with a text box containing '80', 'Server Access' with a dropdown menu showing 'WLAN & LAN', and 'Secured Client IP Address' with radio buttons for 'All' (selected) and 'Selected', followed by a text box containing '0.0.0.0'. Under 'HTTPS', there are five settings: 'Server Certificate' with a dropdown menu showing 'auto\_generated\_self\_signed\_cert' and a link '(See My Certificates)', a checkbox for 'Authenticate Client Certificates (See Trusted CAs)', 'Server Port' with a text box containing '443', 'Server Access' with a dropdown menu showing 'WLAN & LAN', and 'Secured Client IP Address' with radio buttons for 'All' (selected) and 'Selected', followed by a text box containing '0.0.0.0'. At the bottom, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

**Table 48** Remote Management: WWW

| LABEL                            | DESCRIPTION  |
|----------------------------------|--|
| WWW                              |  |
| Server Port                      | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.   |
| Server Access                    | Select the interface(s) through which a computer may access the ZyXEL Device using this service.   |
| Secured Client IP Address        | A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service.<br>Select <b>All</b> to allow any computer to access the ZyXEL Device using this service.<br>Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.                   |
| HTTPS                            |  |
| Server Certificate               | Select the <b>Server Certificate</b> that the ZyXEL Device will use to identify itself. The ZyXEL Device is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyXEL Device).   |
| Authenticate Client Certificates | Select <b>Authenticate Client Certificates</b> (optional) to require the SSL client to authenticate itself with the ZyXEL Device by sending the ZyXEL Device a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ZyXEL Device (see the appendix on importing certificates for details). |
| Server Port                      | The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the ZyXEL Device, for example 8443, then you must notify people who need to access the ZyXEL Device web configurator to use "https://ZyXEL Device IP Address: <b>8443</b> " as the URL.  |

**Table 48** Remote Management: WWW

| LABEL                     | DESCRIPTION   |
|---------------------------|---|
| Server Access             | Select a ZyXEL Device interface from <b>Server Access</b> on which incoming HTTPS access is allowed.<br>You can allow only secure web configurator access by setting the <b>WWW Server Access</b> field to <b>Disable</b> and setting the <b>HTTPS Server Access</b> field to an interface(s).  |
| Secured Client IP Address | A secure client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service.<br>Select <b>All</b> to allow any computer to access the ZyXEL Device using this service.<br>Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service. |
| Apply                     | Click <b>Apply</b> to save your customized settings and exit this screen.   |
| Reset                     | Click <b>Reset</b> to begin configuring this screen afresh.   |

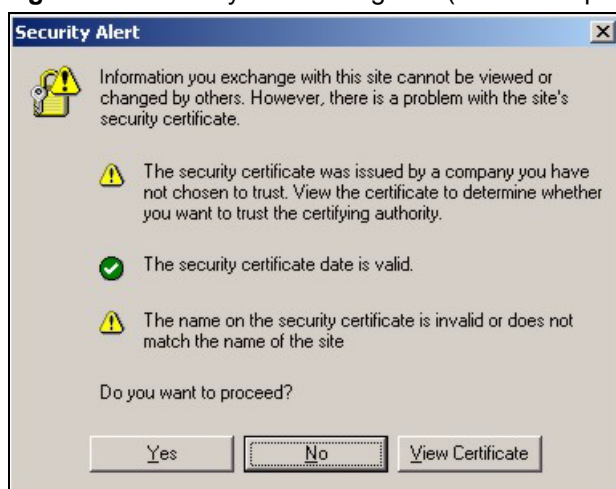
## 12.9 HTTPS Example

If you haven’t changed the default HTTPS port on the ZyXEL Device, then in your browser enter “https://ZyXEL Device IP Address/” as the web site address where “ZyXEL Device IP Address” is the IP address or domain name of the ZyXEL Device you wish to access.

### 12.9.1 Internet Explorer Warning Messages

When you attempt to access the ZyXEL Device HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the ZyXEL Device.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

**Figure 86** Security Alert Dialog Box (Internet Explorer)

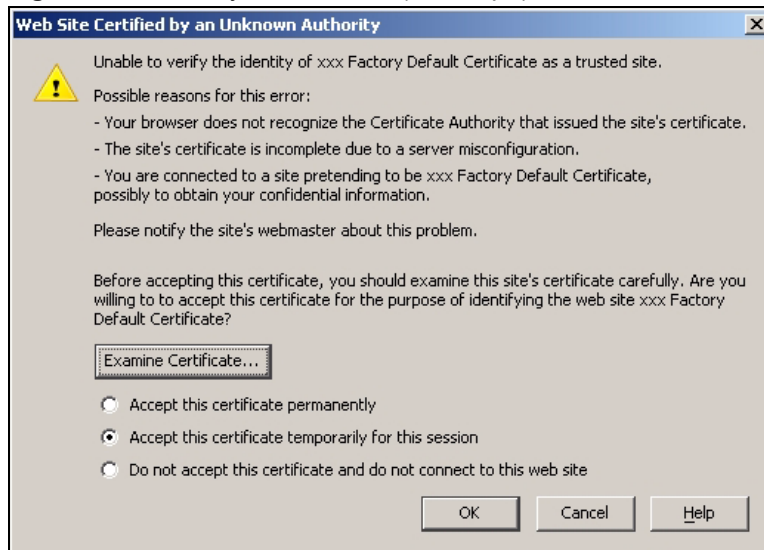
## 12.9.2 Netscape Navigator Warning Messages

When you attempt to access the ZyXEL Device HTTPS server, a **Website Certified by an Unknown Authority** screen pops up asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the ZyXEL Device.

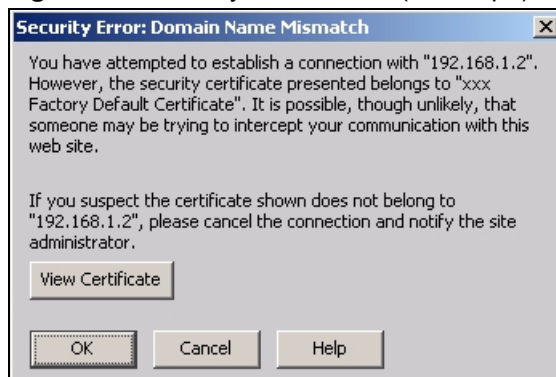
If **Accept this certificate temporarily for this session** is selected, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the ZyXEL Device's certificate into the SSL client.

**Figure 87** Security Certificate 1 (Netscape)



**Figure 88** Security Certificate 2 (Netscape)



## 12.9.3 Avoiding the Browser Warning Messages

The following describes the main reasons that your browser displays warnings about the ZyXEL Device's HTTPS server certificate and what you can do to avoid seeing the warnings.

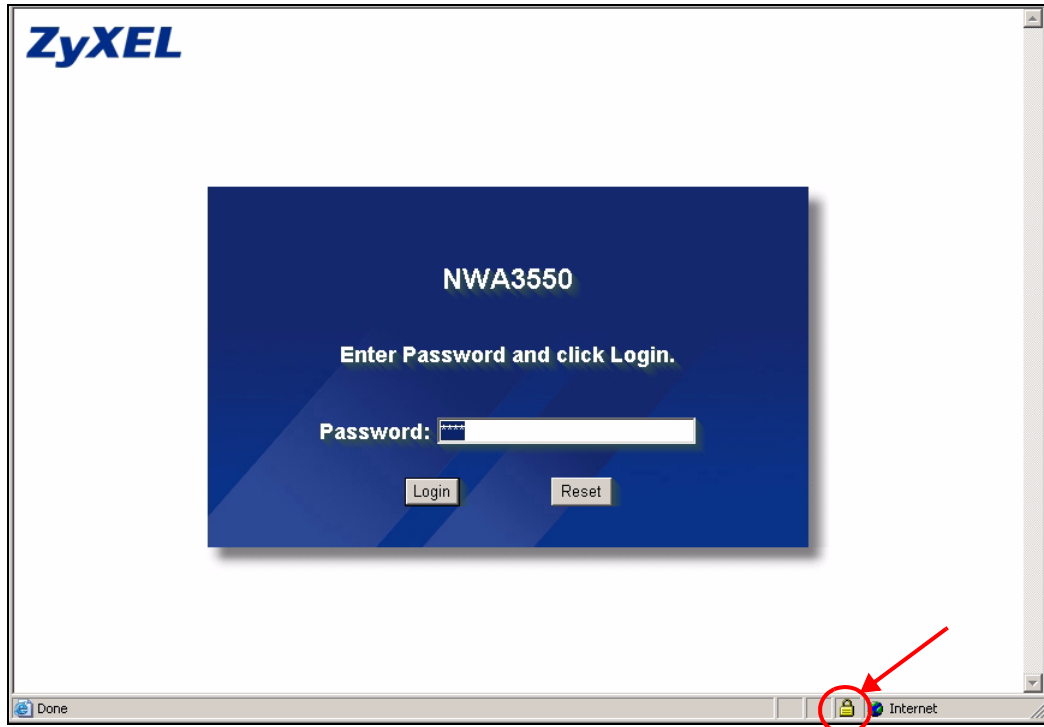
- The issuing certificate authority of the ZyXEL Device's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the ZyXEL Device's factory default certificate is the ZyXEL Device itself since the certificate is a self-signed certificate.
  - For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
  - To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate. Refer to [Appendix F on page 755](#) for details.
- The actual IP address of the HTTPS server (the IP address of the ZyXEL Device's port that you are trying to access) does not match the common name specified in the ZyXEL Device's HTTPS server certificate that your browser received. Do the following to check the common name specified in the certificate that your ZyXEL Device sends to HTTPS clients.
  - 2a** Click **REMOTE MGMT**. Write down the name of the certificate displayed in the **Server Certificate** field.
  - 2b** Click **CERTIFICATES**. Find the certificate and check its **Subject** column. CN stands for certificate's common name (see [Figure 91 on page 154](#) for an example).

Use this procedure to have the ZyXEL Device use a certificate with a common name that matches the ZyXEL Device's actual IP address. You cannot use this procedure if you need to access the WAN port and it uses a dynamically assigned IP address.

- 2a** Create a new certificate for the ZyXEL Device that uses the IP address (of the ZyXEL Device's port that you are trying to access) as the certificate's common name. For example, to use HTTPS to access a LAN port with IP address 192.168.1.2, create a certificate that uses 192.168.1.2 as the common name.
- 2b** Go to the remote management **WWW** screen and select the newly created certificate in the **Server Certificate** field. Click **Apply**.

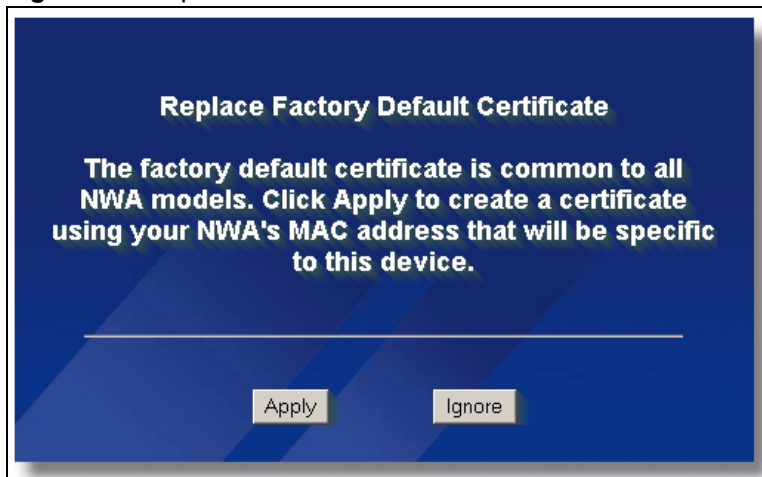
## 12.9.4 Login Screen

After you accept the certificate, the ZyXEL Device login screen appears. The lock displayed in the bottom right of the browser status bar denotes a secure connection.

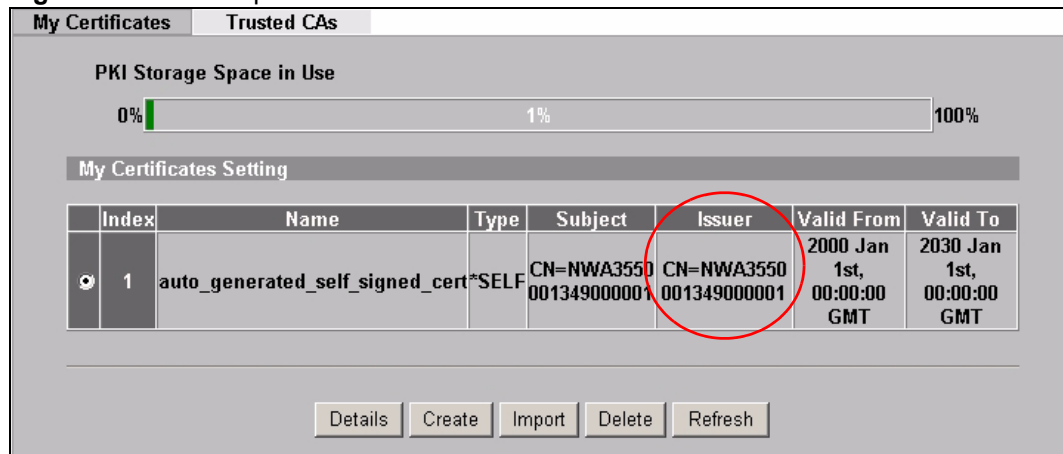
**Figure 89** Example: Lock Denoting a Secure Connection

Click **Login** and you then see the next screen.

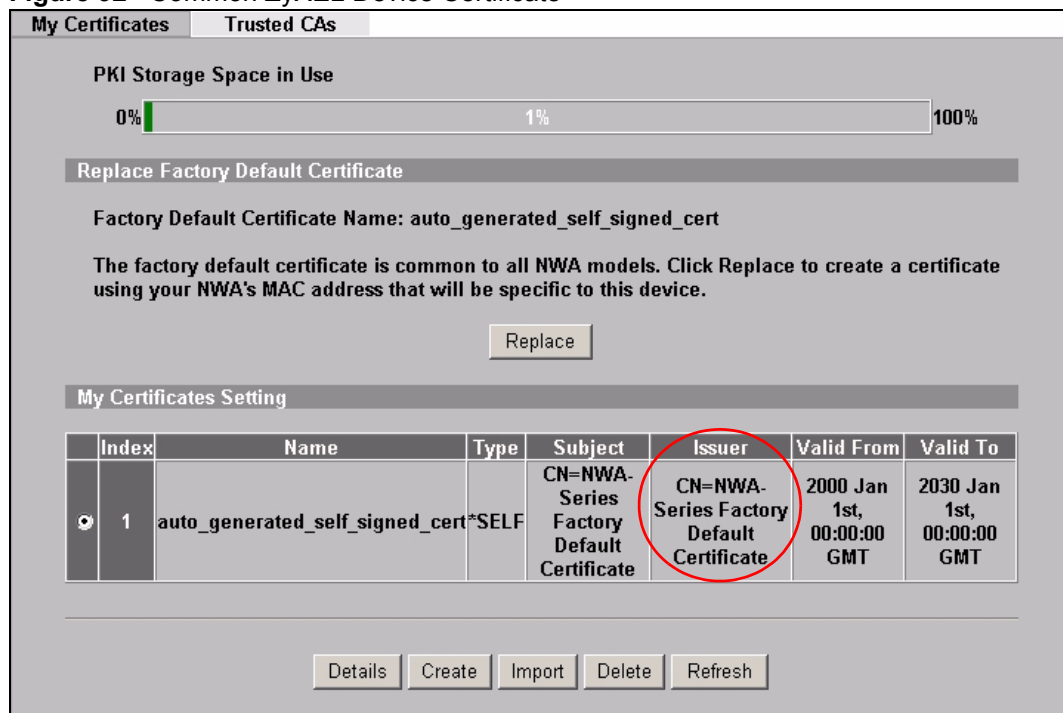
The factory default certificate is a common default certificate for all ZyXEL Device models.

**Figure 90** Replace Certificate

Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyXEL Device's MAC address that will be specific to this device. Click **CERTIFICATES** to open the **My Certificates** screen. You will see information similar to that shown in the following figure.

**Figure 91** Device-specific Certificate

Click **Ignore** in the **Replace Certificate** screen to use the common ZyXEL Device certificate. You will then see this information in the **My Certificates** screen.

**Figure 92** Common ZyXEL Device Certificate

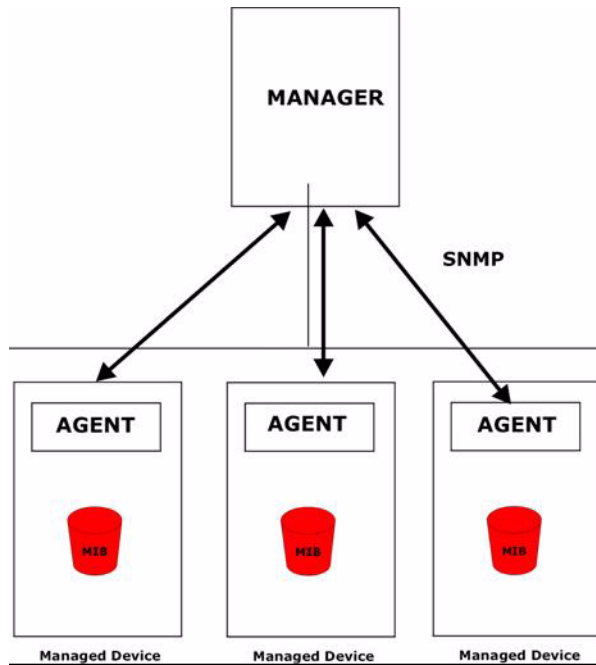
## 12.10 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyXEL Device supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1), version two (SNMPv2c), and version 3 (SNMPv3), at the time of writing. The next figure illustrates an SNMP management operation.



SNMP is available only if TCP/IP is configured.

**Figure 93** SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyXEL Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

## 12.10.1 Supported MIBs

The ZyXEL Device supports MIB II that is defined in RFC-1213 and RFC-1215 as well as the proprietary ZyXEL private MIB. The purpose of the MIBs is to let administrators collect statistical data and monitor status and performance.

## 12.10.2 SNMP Traps

The ZyXEL Device can send the following traps to the SNMP manager.

**Table 49** SNMP Traps

| TRAP NAME  | OBJECT IDENTIFIER # (OID)  | DESCRIPTION  |
|--|----------------------------|--|
| Generic Traps  |                            |  |
| coldStart  | 1.3.6.1.6.3.1.1.5.1        | This trap is sent after booting (power on). This trap is defined in RFC-1215.  |
| warmStart  | 1.3.6.1.6.3.1.1.5.2        | This trap is sent after booting (software reboot). This trap is defined in RFC-1215.   |
| linkDown   | 1.3.6.1.6.3.1.1.5.3        | This trap is sent when the Ethernet link is down.  |
| linkUp   | 1.3.6.1.6.3.1.1.5.4        | This trap is sent when the Ethernet link is up.  |
| authenticationFailure<br>(defined in <i>RFC-1215</i> ) | 1.3.6.1.6.3.1.1.5.5        | The device sends this trap when it receives any SNMP get or set requirements with the wrong community (password).<br><br>Note: snmpEnableAuthenTraps, OID 1.3.6.1.2.1.11.30 (defined in RFC 1214 and RFC 1907) must be enabled on in order for the device to send authenticationFailure traps. Use a MIB browser to enable or disable snmpEnableAuthenTraps. |
| Traps defined in the ZyXEL Private MIB.                |                            |  |
| whyReboot  | 1.3.6.1.4.1.890.1.5.13.0.1 | This trap is sent with the reason for restarting before the system reboots (warm start). "System reboot by user!" is added for an intentional reboot (for example, download new files, CI command "sys reboot"). If the system reboots because of fatal errors, a code for the error is listed.  |
| pwTrapWirelessStatus                                   | 1.3.6.1.4.1.890.1.9.2.1.1  | This is to enable or disable the wireless group trap.  |
| pwWlanStaAssociation                                   | 1.3.6.1.4.1.890.9.2.3.1.1  | This trap is sent when a wireless station associates with the ZyXEL Device.  |
| pwWlanStaDisassociation                                | 1.3.6.1.4.1.890.9.2.3.1.2  | This trap is sent when a wireless station disconnects from the ZyXEL Device.   |
| pwTrapSecurityStatus                                   | 1.3.6.1.4.1.890.1.9.2.1.2  | This is to enable or disable the security group trap.  |
| pwWlanStaAuthFail                                      | 1.3.6.1.4.1.890.9.2.3.2.1  | This trap is sent when a wireless station fails to authenticate with the ZyXEL Device.   |

**Table 49** SNMP Traps

| TRAP NAME        | OBJECT IDENTIFIER # (OID) | DESCRIPTION  |
|------------------|---------------------------|--|
| pwTrapTFTPStatus | 1.3.6.1.4.1.890.1.9.2.1.3 | This is to enable or disable the TFTP group trap.  |
| pwTFTPStatus     | 1.3.6.1.4.1.890.9.2.3.3.1 | This trap is sent to indicate the status and result of a TFTP client session that has ended. |

## 12.11 SNMP Trap Interface Index

Some traps include an SNMP interface index. The following table maps the SNMP interface indexes to the ZyXEL Device's physical and virtual ports.

**Table 50** SNMP Interface Index to Physical and Virtual Port Mapping

| TYPE     | INTERFACE       | PORT                       |
|----------|-----------------|----------------------------|
| Physical | enet0           | Wireless LAN adaptor WLAN1 |
|          | enet1           | Ethernet port (LAN)        |
|          | enet2           | Wireless LAN adaptor WLAN2 |
| Virtual  | enet3 ~ enet9   | WLAN1 in MBSSID mode       |
|          | enet10 ~ enet16 | WLAN2 in MBSSID mode       |
|          | enet17 ~ enet21 | WLAN1 in WDS mode          |
|          | enet22 ~ enet26 | WLAN2 in WDS mode          |

### 12.11.1 SNMP v3 and Security

SNMP v3 enhances security for SNMP management. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

### 12.11.2 Configuring SNMP

To change your ZyXEL Device's SNMP settings, click **REMOTE MGNT > SNMP**. The screen appears as shown.

**Figure 94** Remote Management: SNMP

TELNET FTP WWW **SNMP**

**SNMP Configuration**

Get Community

Set Community

Trap Destination

SNMP Version

Trap Community

User Profile

[Configure SNMPv3 User Profile](#)

**SNMP**

Service Port

Service Access

Secured Client IP Address ☒ All ☐ Selected

The following table describes the labels in this screen.

**Table 51** Remote Management: SNMP

| LABEL                         | DESCRIPTION  |
|-------------------------------|--|
| SNMP Configuration            |  |
| Get Community                 | Enter the <b>Get Community</b> , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.   |
| Set Community                 | Enter the <b>Set Community</b> , which is the password for incoming Set requests from the management station. The default is public and allows all requests.   |
| Trap Destination              | Type the IP address of the station to send your SNMP traps to.   |
| SNMP Version                  | Select the SNMP version for the ZyXEL Device. The SNMP version on the ZyXEL Device must match the version on the SNMP manager. Choose SNMP version 1 ( <b>SNMPv1</b> ), SNMP version 2 ( <b>SNMPv2</b> ) or SNMP version 3 ( <b>SNMPv3</b> ).  |
| Trap Community                | Type the trap community, which is the password sent with each trap to the SNMP manager. The default is "public" and allows all requests.<br>This field is available only when <b>SNMPv1</b> or <b>SNMPv2</b> is selected in the <b>SNMP Version</b> field.   |
| User Profile                  | This field is available only when you select <b>SNMPv3</b> in the <b>SNMP Version</b> field. When sending SNMP v3 traps (messages sent independently by the SNMP agent) the agent must authenticate the SNMP manager. If the SNMP manager does not provide the correct security details, the agent does not send the traps. The ZyXEL Device has two SNMP version 3 login accounts, <b>User</b> and <b>Admin</b> . Each account has different security settings. You can use either account's security settings for authenticating SNMP traps. Select <b>User</b> to have the ZyXEL Device use the <b>User</b> account's security settings, or select <b>Admin</b> to have the ZyXEL Device use the <b>Admin</b> account's security settings. Use the <b>Configure SNNMPv3 User Profile</b> link to set up each account's security settings. |
| Configure SNMPv3 User Profile | Click this to go to the <b>SNMPv3 User Profile</b> screen, where you can configure administration and user login details.  |

**Table 51** Remote Management: SNMP

| LABEL                     | DESCRIPTION   |
|---------------------------|---|
| SNMP                      |   |
| Service Port              | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.  |
| Service Access            | Select the interface(s) through which a computer may access the ZyXEL Device using this service.  |
| Secured Client IP Address | A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service.<br>Select <b>All</b> to allow any computer to access the ZyXEL Device using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service. |
| Apply                     | Click <b>Apply</b> to save your customized settings and exit this screen.   |
| Reset                     | Click <b>Reset</b> to begin configuring this screen afresh.   |

### 12.11.2.1 The SNMPv3 User Profile Screen

Use this screen to set up the details of SNMPv3 users. Click **Configure SNMPv3 User Profile** in the **REMOTE MGNT > SNMP** screen. The following screen displays.

**Figure 95** Remote Management: SNMPv3 User Profile

The screenshot shows the 'SNMPv3 User Profile' configuration screen. It is divided into two main sections: 'SNMPv3Admin' and 'SNMPv3User'. Each section contains the following fields:

- ☒ Enable SNMPv3Admin / Enable SNMPv3User
- User Name: SNMPv3Admin / SNMPv3User
- Password: [masked]
- Confirm Password: [masked]
- Access Type: Set / Get
- Authentication Protocol: MD5
- Privacy Protocol: None

At the bottom of the screen are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

**Table 52** Remote Management: SNMP User Profile

| LABEL              | DESCRIPTION   |
|--------------------|---|
| Enable SNMPv3Admin | Select this box to activate the SNMPv3 administration account. The SNMPv3 administrator can issue Get and Set commands to the ZyXEL Device. |
| User Name          | Enter a username for the SNMPv3 administrator. Only SNMP commands carrying this username are allowed to administer the ZyXEL Device.        |
| Password           | Enter a password for the SNMPv3 administrator. Only SNMP commands carrying this password are allowed to administer the ZyXEL Device.        |

**Table 52** Remote Management: SNMP User Profile

| <b>LABEL</b>            | <b>DESCRIPTION</b>   |
|-------------------------|--|
| Confirm Password        | Re-enter the <b>Password</b> .   |
| Access Type             | For the administrator, this is always <b>Set</b> . SNMP Set commands allow the administrator to make configuration changes.  |
| Authentication Protocol | Select an authentication algorithm. <b>MD5</b> (Message Digest 5) and <b>SHA</b> (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.  |
| Privacy Protocol        | Specify the encryption method for SNMP communication with this user. You can choose one of the following: <ul style="list-style-type: none"> <li>• <b>DES</b> - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data.</li> <li>• <b>AES</b> - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.</li> <li>• <b>None</b> - no encryption is used.</li> </ul> |
| Enable SNMPv3User       | Select this box to activate the SNMPv3 user account. The SNMPv3 user can issue GET commands to the ZyXEL Device.   |
| User Name               | Enter a username for the SNMPv3 user. Only SNMP commands carrying this username are allowed to get details about the ZyXEL Device.   |
| Password                | Enter a password for the SNMPv3 administrator. Only SNMP commands carrying this password are allowed to get details about the ZyXEL Device.  |
| Confirm Password        | Re-enter the <b>Password</b> .   |
| Access Type             | For the administrator, this is always <b>Get</b> . SNMP Get commands allow the user to make see configuration details about the ZyXEL Device.  |
| Authentication Protocol | Select an authentication algorithm. <b>MD5</b> (Message Digest 5) and <b>SHA</b> (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.  |
| Privacy Protocol        | Specify the encryption method for SNMP communication with this user. You can choose one of the following: <ul style="list-style-type: none"> <li>• <b>DES</b> - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data.</li> <li>• <b>AES</b> - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.</li> <li>• <b>None</b> - no encryption is used.</li> </ul> |
| Apply                   | Click <b>Apply</b> to save your customized settings and exit this screen.  |
| Reset                   | Click <b>Reset</b> to begin configuring this screen afresh.  |

# Internal RADIUS Server

The ZyXEL Device can use its internal RADIUS server to authenticate wireless clients. It can also serve as a RADIUS server to authenticate other APs and their wireless clients. For more background information on RADIUS, see [Section 7.4 on page 111](#).

## 13.1 Internal RADIUS Overview

The ZyXEL Device has a built-in RADIUS server that can authenticate wireless clients or other trusted APs.

The ZyXEL Device can function as an AP and as a RADIUS server at the same time.

PEAP (Protected EAP) and MD5 authentication is implemented on the internal RADIUS server using simple username and password methods over a secure TLS connection. See the appendices for more information on the types of EAP authentication and the internal RADIUS authentication method used in your ZyXEL Device.

- Use the **AUTH. SERVER > Setting** screen to turn the ZyAIR's internal RADIUS server off or on and to view information about the ZyXEL Device's certificates.
- Use the **AUTH. SERVER > Trusted AP** screen to specify APs as trusted. Trusted APs can use the ZyAIR's internal RADIUS server to authenticate wireless clients.
- Use the **AUTH. SERVER > Trusted Users** screen to configure a list of wireless client user names and passwords for the ZyAIR to authenticate.

## 13.2 Internal RADIUS Server Setting

The **AUTH. SERVER > Setting** screen displays information about certificates. The certificates are used by wireless clients to authenticate the RADIUS server. Information matching the certificate is held on the wireless client's utility. A password and user name on the utility must match the **Trusted Users** list so that the RADIUS server can be authenticated.



The internal RADIUS server does not support domain accounts (DOMAIN/user). When you configure your Windows XP SP2 Wireless Zero Configuration PEAP/MS-CHAPv2 settings, deselect the Use Windows logon name and password check box. When authentication begins, a pop-up dialog box requests you to type a Name, Password and Domain of the RADIUS server. Specify a name and password only, do not specify a domain.

Click **AUTH. SERVER > Setting**. The screen appears as shown.

**Figure 96** Internal RADIUS Server Setting Screen

| Setting                                    | Trusted AP                      | Trusted Users |                          |                          |                            |                            |
|--|---------------------------------|---------------|--------------------------|--------------------------|----------------------------|----------------------------|
| <input checked="" type="checkbox"/> Active |                                 |               |                          |                          |                            |                            |
| Index                                      | Name                            | Type          | Subject                  | Issuer                   | Valid From                 | Valid To                   |
| 1  | auto_generated_self_signed_cert | *SELF         | CN=NWA3550, 001349000001 | CN=NWA3550, 001349000001 | Jan 1st, 2000 00:00:00 GMT | Jan 1st, 2030 00:00:00 GMT |

Apply Reset

The following table describes the labels in this screen.

**Table 53** Internal RADIUS Server Setting Screen Setting

| LABEL  | DESCRIPTION   |
|--------|---|
| Active | Select the <b>Active</b> check box to have the ZyXEL Device use its internal RADIUS server to authenticate wireless clients or other APs.   |
| Index  | This field displays the certificate index number. The certificates are listed in alphabetical order. Use the <b>CERTIFICATES</b> screens to manage certificates. The internal RADIUS server uses one of the certificates listed in this screen to authenticate each wireless client. The exact certificate used depends on the certificate information configured on the wireless client.   |
| Name   | <p>This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.</p> <p><b>auto_generated_self_signed_cert</b> is the factory default certificate common to all ZyXEL Devices that use certificates.</p> <p>Note: It is recommended that you replace the factory default certificate with one that uses your ZyXEL Device's MAC address. Do this when you first log in to the ZyXEL Device or in the <b>CERTIFICATES &gt; My Certificates</b> screen.</p> |

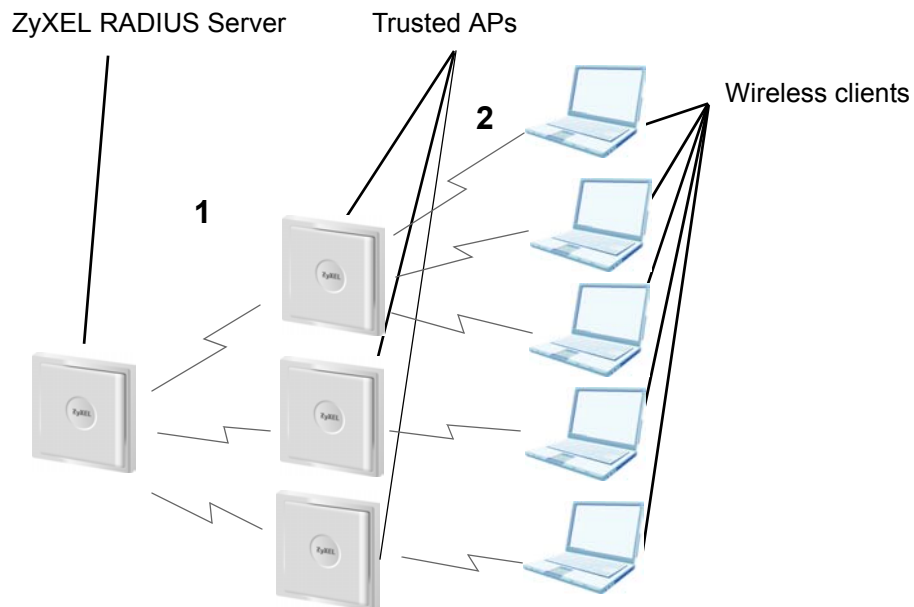
**Table 53** Internal RADIUS Server Setting Screen Setting (continued)

| LABEL      | DESCRIPTION  |
|------------|--|
| Type       | This field displays what kind of certificate this is.<br><b>REQ</b> represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the <b>My Certificate Import</b> screen to import the certificate and replace the request.<br><b>SELF</b> represents a self-signed certificate.<br><b>*SELF</b> represents the default self-signed certificate, which the ZyXEL Device uses to sign imported trusted remote host certificates.<br><b>CERT</b> represents a certificate issued by a certification authority. |
| Subject    | This field displays identifying information about the certificate's owner, such as <b>CN</b> (Common Name), <b>OU</b> (Organizational Unit or department), <b>O</b> (Organization or company) and <b>C</b> (Country). It is recommended that each certificate have unique subject information.   |
| Issuer     | This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the <b>Subject</b> field.  |
| Valid From | This field displays the date that the certificate becomes applicable. The text displays in red and includes a <b>Not Yet Valid!</b> message if the certificate has not yet become applicable.  |
| Valid To   | This field displays the date that the certificate expires. The text displays in red and includes an <b>Expiring!</b> or <b>Expired!</b> message if the certificate is about to expire or has already expired.  |
| Apply      | Click <b>Apply</b> to have the ZyXEL Device use certificates to authenticate wireless clients.   |
| Reset      | Click <b>Reset</b> to start configuring this screen afresh.  |

## 13.3 Trusted AP Overview

A trusted AP is an AP that uses the ZyXEL Device's internal RADIUS server to authenticate its wireless clients. Each wireless client must have a user name and password configured in the **AUTH. SERVER > Trusted Users** screen.

The following figure shows how this is done in two phases.

**Figure 97** Trusted AP Overview

- 1** Configure an IP address and shared secret in the **Trusted AP** database to authenticate an AP as a trusted AP.
- 2** Configure wireless client user names and passwords in the **Trusted Users** database to use a trusted AP as a relay between the ZyXEL Device's internal RADIUS server and the wireless clients. The wireless clients can then be authenticated by the ZyXEL Device's internal RADIUS server.

## 13.4 Configuring Trusted AP

To specify trusted APs, click the **AUTH SERVER** link under **ADVANCED** and then the **Trusted AP** tab. The screen appears as shown.

**Figure 98** Trusted AP Screen

| Setting |                                     | Trusted AP |               | Trusted Users |  |
|---------|-------------------------------------|------------|---------------|---------------|--|
| Index   | Active                              | IP Address | Shared Secret |               |  |
| 1       | <input checked="" type="checkbox"/> | 127.0.0.1  | ****          |               |  |
| 2       | <input type="checkbox"/>            | 0.0.0.0    |               |               |  |
| 3       | <input type="checkbox"/>            | 0.0.0.0    |               |               |  |
| 4       | <input type="checkbox"/>            | 0.0.0.0    |               |               |  |
| 5       | <input type="checkbox"/>            | 0.0.0.0    |               |               |  |
| 6       | <input type="checkbox"/>            | 0.0.0.0    |               |               |  |
| 7       | <input type="checkbox"/>            | 0.0.0.0    |               |               |  |
| 8       | <input type="checkbox"/>            | 0.0.0.0    |               |               |  |
| 9       | <input type="checkbox"/>            | 0.0.0.0    |               |               |  |
| 10      | <input type="checkbox"/>            | 0.0.0.0    |               |               |  |
| 11      | <input type="checkbox"/>            | 0.0.0.0    |               |               |  |
| 12      | <input type="checkbox"/>            | 0.0.0.0    |               |               |  |
| 13      | <input type="checkbox"/>            | 0.0.0.0    |               |               |  |
| 29      | <input type="checkbox"/>            | 0.0.0.0    |               |               |  |
| 30      | <input type="checkbox"/>            | 0.0.0.0    |               |               |  |
| 31      | <input type="checkbox"/>            | 0.0.0.0    |               |               |  |
| 32      | <input type="checkbox"/>            | 0.0.0.0    |               |               |  |

The following table describes the labels in this screen.

**Table 54** Trusted AP

| LABEL         | DESCRIPTION  |
|---------------|--|
| Index         | This field displays the trusted AP index number.   |
| Active        | Select this check box to have the ZyXEL Device use the <b>IP Address</b> and <b>Shared Secret</b> to authenticate a trusted AP.  |
| IP Address    | Type the IP address of the trusted AP in dotted decimal notation.  |
| Shared Secret | <p>Enter a password (up to 31 alphanumeric characters, no spaces) as the key for encrypting communications between the AP and the ZyXEL Device. The key is not sent over the network. This key must be the same on the AP and the ZyXEL Device. Both the ZyXEL Device's IP address and this shared secret must also be configured in the "external RADIUS" server fields of the trusted AP.</p> <p><b>Note:</b> The first trusted AP fields are for the ZyXEL Device itself.</p> |
| Apply         | Click <b>Apply</b> to save your changes.   |
| Reset         | Click <b>Reset</b> to begin configuring this screen afresh.  |

## 13.5 Configuring Trusted Users

A trusted user entry consists of a wireless client user name and password. To configure trusted user entries, click **AUTH SERVER > Trusted Users**. The screen appears as shown.

**Figure 99** Trusted Users Screen

| Index | Active                   | User Name | Password |
|-------|--------------------------|-----------|----------|
| 1     | <input type="checkbox"/> |           |          |
| 2     | <input type="checkbox"/> |           |          |
| 3     | <input type="checkbox"/> |           |          |
| 4     | <input type="checkbox"/> |           |          |
| 5     | <input type="checkbox"/> |           |          |
| 6     | <input type="checkbox"/> |           |          |
| 7     | <input type="checkbox"/> |           |          |
| 8     | <input type="checkbox"/> |           |          |
| 9     | <input type="checkbox"/> |           |          |
| 10    | <input type="checkbox"/> |           |          |
| 11    | <input type="checkbox"/> |           |          |
| 12    | <input type="checkbox"/> |           |          |
| 13    | <input type="checkbox"/> |           |          |
| 14    | <input type="checkbox"/> |           |          |
| 15    | <input type="checkbox"/> |           |          |
| 16    | <input type="checkbox"/> |           |          |
| 17    | <input type="checkbox"/> |           |          |
| 18    | <input type="checkbox"/> |           |          |
| 19    | <input type="checkbox"/> |           |          |
| 20    | <input type="checkbox"/> |           |          |
| 21    | <input type="checkbox"/> |           |          |
| 22    | <input type="checkbox"/> |           |          |
| 23    | <input type="checkbox"/> |           |          |
| 24    | <input type="checkbox"/> |           |          |
| 25    | <input type="checkbox"/> |           |          |
| 26    | <input type="checkbox"/> |           |          |
| 27    | <input type="checkbox"/> |           |          |
| 28    | <input type="checkbox"/> |           |          |
| 29    | <input type="checkbox"/> |           |          |
| 30    | <input type="checkbox"/> |           |          |
| 31    | <input type="checkbox"/> |           |          |
| 32    | <input type="checkbox"/> |           |          |
| 33    | <input type="checkbox"/> |           |          |
| 34    | <input type="checkbox"/> |           |          |
| 35    | <input type="checkbox"/> |           |          |
| 36    | <input type="checkbox"/> |           |          |
| 37    | <input type="checkbox"/> |           |          |
| 38    | <input type="checkbox"/> |           |          |
| 39    | <input type="checkbox"/> |           |          |
| 40    | <input type="checkbox"/> |           |          |
| 41    | <input type="checkbox"/> |           |          |
| 42    | <input type="checkbox"/> |           |          |
| 43    | <input type="checkbox"/> |           |          |
| 44    | <input type="checkbox"/> |           |          |
| 45    | <input type="checkbox"/> |           |          |
| 46    | <input type="checkbox"/> |           |          |
| 47    | <input type="checkbox"/> |           |          |
| 48    | <input type="checkbox"/> |           |          |
| 49    | <input type="checkbox"/> |           |          |
| 50    | <input type="checkbox"/> |           |          |
| 51    | <input type="checkbox"/> |           |          |
| 52    | <input type="checkbox"/> |           |          |
| 53    | <input type="checkbox"/> |           |          |
| 54    | <input type="checkbox"/> |           |          |
| 55    | <input type="checkbox"/> |           |          |
| 56    | <input type="checkbox"/> |           |          |
| 57    | <input type="checkbox"/> |           |          |
| 58    | <input type="checkbox"/> |           |          |
| 59    | <input type="checkbox"/> |           |          |
| 60    | <input type="checkbox"/> |           |          |
| 61    | <input type="checkbox"/> |           |          |
| 62    | <input type="checkbox"/> |           |          |
| 63    | <input type="checkbox"/> |           |          |
| 64    | <input type="checkbox"/> |           |          |
| 65    | <input type="checkbox"/> |           |          |
| 66    | <input type="checkbox"/> |           |          |
| 67    | <input type="checkbox"/> |           |          |
| 68    | <input type="checkbox"/> |           |          |
| 69    | <input type="checkbox"/> |           |          |
| 70    | <input type="checkbox"/> |           |          |
| 71    | <input type="checkbox"/> |           |          |
| 72    | <input type="checkbox"/> |           |          |
| 73    | <input type="checkbox"/> |           |          |
| 74    | <input type="checkbox"/> |           |          |
| 75    | <input type="checkbox"/> |           |          |
| 76    | <input type="checkbox"/> |           |          |
| 77    | <input type="checkbox"/> |           |          |
| 78    | <input type="checkbox"/> |           |          |
| 79    | <input type="checkbox"/> |           |          |
| 80    | <input type="checkbox"/> |           |          |
| 81    | <input type="checkbox"/> |           |          |
| 82    | <input type="checkbox"/> |           |          |
| 83    | <input type="checkbox"/> |           |          |
| 84    | <input type="checkbox"/> |           |          |
| 85    | <input type="checkbox"/> |           |          |
| 86    | <input type="checkbox"/> |           |          |
| 87    | <input type="checkbox"/> |           |          |
| 88    | <input type="checkbox"/> |           |          |
| 89    | <input type="checkbox"/> |           |          |
| 90    | <input type="checkbox"/> |           |          |
| 91    | <input type="checkbox"/> |           |          |
| 92    | <input type="checkbox"/> |           |          |
| 93    | <input type="checkbox"/> |           |          |
| 94    | <input type="checkbox"/> |           |          |
| 95    | <input type="checkbox"/> |           |          |
| 96    | <input type="checkbox"/> |           |          |
| 97    | <input type="checkbox"/> |           |          |
| 98    | <input type="checkbox"/> |           |          |
| 99    | <input type="checkbox"/> |           |          |
| 100   | <input type="checkbox"/> |           |          |
| 101   | <input type="checkbox"/> |           |          |
| 102   | <input type="checkbox"/> |           |          |
| 103   | <input type="checkbox"/> |           |          |
| 104   | <input type="checkbox"/> |           |          |
| 105   | <input type="checkbox"/> |           |          |
| 106   | <input type="checkbox"/> |           |          |
| 107   | <input type="checkbox"/> |           |          |
| 108   | <input type="checkbox"/> |           |          |
| 109   | <input type="checkbox"/> |           |          |
| 110   | <input type="checkbox"/> |           |          |
| 111   | <input type="checkbox"/> |           |          |
| 112   | <input type="checkbox"/> |           |          |
| 113   | <input type="checkbox"/> |           |          |
| 114   | <input type="checkbox"/> |           |          |
| 115   | <input type="checkbox"/> |           |          |
| 116   | <input type="checkbox"/> |           |          |
| 117   | <input type="checkbox"/> |           |          |
| 118   | <input type="checkbox"/> |           |          |
| 119   | <input type="checkbox"/> |           |          |
| 120   | <input type="checkbox"/> |           |          |
| 121   | <input type="checkbox"/> |           |          |
| 122   | <input type="checkbox"/> |           |          |
| 123   | <input type="checkbox"/> |           |          |
| 124   | <input type="checkbox"/> |           |          |
| 125   | <input type="checkbox"/> |           |          |
| 126   | <input type="checkbox"/> |           |          |
| 127   | <input type="checkbox"/> |           |          |
| 128   | <input type="checkbox"/> |           |          |

Note. Password: Maximum 14 ASCII characters with PEAP

Apply Reset

The following table describes the labels in this screen.

**Table 55** Trusted Users

| LABEL     | DESCRIPTION  |
|-----------|--|
| Index     | This field displays the trusted user index number.   |
| Active    | Select this check box to have the ZyAIR authenticate wireless clients with the same user name and password activated on their wireless utilities.  |
| User Name | Enter the user name for this user account. This name can be up to 31 alphanumeric characters long, including spaces. The wireless client's utility must use this name as its login name. |

**Table 55** Trusted Users

| LABEL    | DESCRIPTION   |
|----------|---|
| Password | <p>Type a password (up to 31 ASCII characters) for this user profile. Note that as you type a password, the screen displays a (*) for each character you type.</p> <p>The password on the wireless client's utility must be the same as this password.</p> <p><b>Note:</b> If you are using PEAP authentication, this password field is limited to 14 ASCII characters in length.</p> |
| Apply    | Click <b>Apply</b> to save your changes.  |
| Reset    | Click <b>Reset</b> to begin configuring this screen afresh.   |



# Certificates

This chapter gives background information about public-key certificates and explains how to use them.

## 14.1 Certificates Overview

The ZyXEL Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyXEL Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

In public-key encryption and decryption, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

- 1 Tim wants to send a private message to Jenny. Tim generates a public key pair. What is encrypted with one key can only be decrypted using the other.
- 2 Tim keeps the private key and makes the public key openly available.
- 3 Tim uses his private key to encrypt the message and sends it to Jenny.
- 4 Jenny receives the message and uses Tim's public key to decrypt it.
- 5 Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The ZyXEL Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyXEL Device does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyXEL Device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

### 14.1.1 Advantages of Certificates

Certificates offer the following benefits.

- The ZyXEL Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

## 14.2 Self-signed Certificates

You can have the ZyXEL Device act as a certification authority and sign its own certificates.

## 14.3 Verifying a Certificate

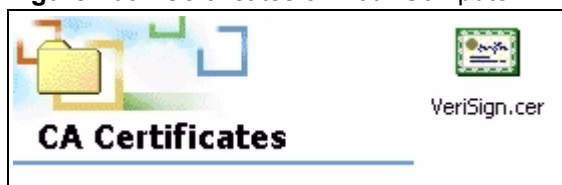
Before you import a trusted CA certificate into the ZyXEL Device, you should verify that you have the actual certificate. This is especially important since the ZyXEL Device also trusts any valid certificate signed by any of the imported trusted CA certificates.

### 14.3.1 Checking the Fingerprint of a Certificate on Your Computer

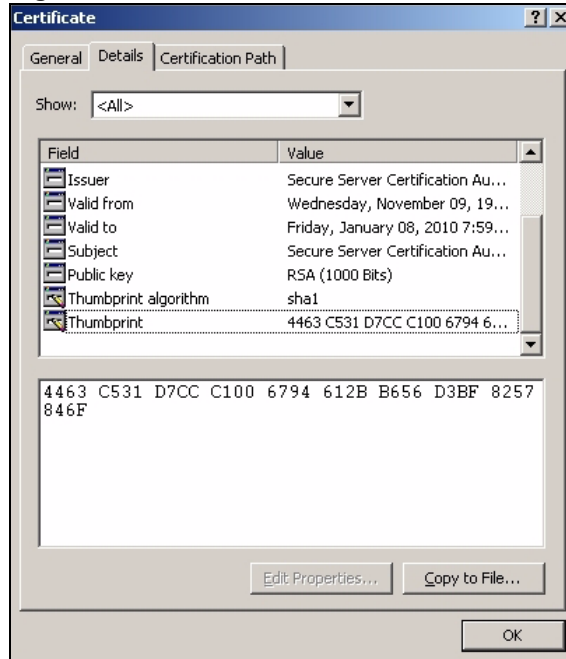
A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

- 1 Browse to where you have the certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

**Figure 100** Certificates on Your Computer



- 3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

**Figure 101** Certificate Details

- 4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may vary according to your situation. Possible examples would be over the telephone or through an HTTPS connection.

## 14.4 Configuration Summary

This section summarizes how to manage certificates.

Use the **My Certificate** screens to generate and export self-signed certificates or certification requests and import the ZyXEL Devices' CA-signed certificates.

Use the **Trusted CA** screens to save CA certificates to the ZyXEL Device.

## 14.5 My Certificates

Click **CERTIFICATES > My Certificates** to open the ZyXEL Device's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray. See the following figure.

**Figure 102** My Certificates

**My Certificates**    **Trusted CAs**

**PKI Storage Space in Use**

0%  1% 100%

**Replace Factory Default Certificate**

Factory Default Certificate Name: auto\_generated\_self\_signed\_cert

The factory default certificate is common to all NWA models. Click Replace to create a certificate using your NWA's MAC address that will be specific to this device.

**My Certificates Setting**

|                                  | Index | Name                            | Type  | Subject                                   | Issuer                                    | Valid From                 | Valid To                   |
|----------------------------------|-------|---------------------------------|-------|---|---|----------------------------|----------------------------|
| <input checked="" type="radio"/> | 1     | auto_generated_self_signed_cert | *SELF | CN=NWA-Series Factory Default Certificate | CN=NWA-Series Factory Default Certificate | 2000 Jan 1st, 00:00:00 GMT | 2030 Jan 1st, 00:00:00 GMT |

The following table describes the labels in this screen.

**Table 56** My Certificates

| LABEL                    | DESCRIPTION   |
|--------------------------|---|
| PKI Storage Space in Use | This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.   |
| Replace                  | This button displays when the ZyXEL Device has the factory default certificate. The factory default certificate is common to all ZyXEL Devices that use certificates. ZyXEL recommends that you use this button to replace the factory default certificate with one that uses your ZyXEL Device's MAC address.  |
| Index                    | This field displays the certificate index number. The certificates are listed in alphabetical order.  |
| Name                     | This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.   |
| Type                     | <p>This field displays what kind of certificate this is.</p> <p><b>REQ</b> represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the <b>My Certificate Import</b> screen to import the certificate and replace the request.</p> <p><b>SELF</b> represents a self-signed certificate.</p> <p><b>*SELF</b> represents the default self-signed certificate, which the ZyXEL Device uses to sign imported trusted remote host certificates.</p> <p><b>CERT</b> represents a certificate issued by a certification authority.</p> |
| Subject                  | This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.  |

**Table 56** My Certificates (continued)

| LABEL      | DESCRIPTION  |
|------------|--|
| Issuer     | This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the <b>Subject</b> field.  |
| Valid From | This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.   |
| Valid To   | This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.  |
| Details    | <p>Click the details icon to open a screen with an in-depth list of information about the certificate.</p> <p>Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate.</p> <p>You cannot delete a certificate that one or more features is configured to use.</p> <p>Do the following to delete a certificate that shows <b>*SELF</b> in the <b>Type</b> field.</p> <ol style="list-style-type: none"> <li>1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the <b>*SELF</b> certificate.</li> <li>2. Click the details icon next to another self-signed certificate (see the description on the <b>Create</b> button if you need to create a self-signed certificate).</li> <li>3. Select the <b>Default self-signed certificate which signs the imported remote host certificates</b> check box.</li> <li>4. Click <b>Apply</b> to save the changes and return to the <b>My Certificates</b> screen.</li> <li>5. The certificate that originally showed <b>*SELF</b> displays <b>SELF</b> and you can delete it now.</li> </ol> <p>Note that subsequent certificates move up by one when you take this action</p> |
| Create     | Click <b>Create</b> to go to the screen where you can have the ZyXEL Device generate a certificate or a certification request.   |
| Import     | Click <b>Import</b> to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the ZyXEL Device.  |
| Delete     | Click <b>Delete</b> to delete an existing certificate. A window display asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.   |
| Refresh    | Click <b>Refresh</b> to display the current validity status of the certificates.   |

## 14.6 Certificate File Formats

The certification authority certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The ZyXEL Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

## 14.7 Importing a Certificate

Click **CERTIFICATES > My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the ZyXEL Device.



You can import only a certificate that matches a corresponding certification request that was generated by the ZyXEL Device.



The certificate you import replaces the corresponding request in the My Certificates screen.



You must remove any spaces from the certificate's filename before you can import it.

**Figure 103** My Certificate Import

**Import**

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on NWA. After the importation, the certification request will automatically be deleted.

File Path:

The following table describes the labels in this screen.

**Table 57** My Certificate Import

| LABEL     | DESCRIPTION  |
|-----------|--|
| File Path | Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it. |
| Browse    | Click <b>Browse</b> to find the certificate file you want to upload.                                 |
| Apply     | Click <b>Apply</b> to save the certificate on the ZyXEL Device.                                      |
| Cancel    | Click <b>Cancel</b> to quit and return to the <b>My Certificates</b> screen.                         |

## 14.8 Creating a Certificate

Click **CERTIFICATES > My Certificates** and then **Create** to open the **My Certificate Create** screen. Use this screen to have the ZyXEL Device create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request, see the following figure.

**Figure 104** My Certificate Create

The screenshot shows the 'My Certificate Create' web interface. At the top, there is a 'Certificate Name' text input field. Below it is a section titled 'Subject Information' with a grey header. This section contains several fields: 'Common Name' with three radio button options ('Host IP Address' selected, 'Host Domain Name', and 'E-Mail'), each followed by a text input field; 'Organizational Unit', 'Organization', and 'Country', each with a text input field; and 'Key Length' with a dropdown menu set to '1024' and the unit 'bits'. Below the 'Subject Information' section is another section titled 'Enrollment Options' with a grey header. This section contains three radio button options: 'Create a self-signed certificate' (selected), 'Create a certification request and save it locally for later manual enrollment', and 'Create a certification request and enroll for a certificate immediately online'. Below these are fields for 'Enrollment Protocol' (a dropdown menu set to 'Simple Certificate Enrollment Protocol (SCEP)'), 'CA Server Address' (a text input field), 'CA Certificate' (a checkbox labeled '(See [Trusted CAs](#))'), 'Request Authentication' (a text input field), 'Reference Number' (a text input field), and 'Key' (a text input field). At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

**Table 58** My Certificate Create

| LABEL  | DESCRIPTION  |
|--|--|
| Certificate Name   | Type up to 31 ASCII characters (not including spaces) to identify this certificate.  |
| Subject Information  | Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the <b>Common Name</b> is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.  |
| Common Name  | Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.  |
| Organizational Unit  | Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.   |
| Organization   | Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.  |
| Country  | Type up to 127 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.  |
| Key Length   | Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.   |
| Enrollment Options   | These radio buttons deal with how and when the certificate is to be generated.   |
| Create a self-signed certificate   | Select <b>Create a self-signed certificate</b> to have the ZyXEL Device generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.  |
| Create a certification request and save it locally for later manual enrollment | Select <b>Create a certification request and save it locally for later manual enrollment</b> to have the ZyXEL Device generate and store a request for a certificate. Use the <b>My Certificate Details</b> screen to view the certification request and copy it to send to the certification authority.<br>Copy the certification request from the <b>My Certificate Details</b> screen ( <a href="#">Section 14.9 on page 177</a> ) and then send it to the certification authority.   |
| Create a certification request and enroll for a certificate immediately online | Select <b>Create a certification request and enroll for a certificate immediately online</b> to have the ZyXEL Device generate a request for a certificate and apply to a certification authority for a certificate.<br>You must have the certification authority's certificate already imported in the <b>Trusted CAs</b> screen.<br>When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the <b>Reference Number</b> and <b>Key</b> if the certification authority requires them. |
| Enrollment Protocol  | Select the certification authority's enrollment protocol from the drop-down list box.<br><b>Simple Certificate Enrollment Protocol (SCEP)</b> is a TCP-based enrollment protocol that was developed by VeriSign and Cisco.<br><b>Certificate Management Protocol (CMP)</b> is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.  |

**Table 58** My Certificate Create (continued)

| LABEL                  | DESCRIPTION   |
|------------------------|---|
| CA Server Address      | Enter the IP address (or URL) of the certification authority server.  |
| CA Certificate         | Select the certification authority's certificate from the <b>CA Certificate</b> drop-down list box.<br>You must have the certification authority's certificate already imported in the <b>Trusted CAs</b> screen. Click <b>Trusted CAs</b> to go to the <b>Trusted CAs</b> screen where you can view (and manage) the ZyXEL Device's list of certificates of trusted certification authorities.   |
| Request Authentication | When you select <b>Create a certification request and enroll for a certificate immediately online</b> , the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the <b>Reference Number</b> and the <b>Key</b> fields if your certification authority uses CMP enrollment protocol. Just fill in the <b>Key</b> field if your certification authority uses the SECP enrollment protocol. |
| Key                    | Type the key that the certification authority gave you.   |
| Apply                  | Click <b>Apply</b> to begin certificate or certification request generation.  |
| Cancel                 | Click <b>Cancel</b> to quit and return to the <b>My Certificates</b> screen.  |

After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the ZyXEL Device is generating the self-signed certificate or certification request.

After the ZyXEL Device successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the ZyXEL Device enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the ZyXEL Device to enroll a certificate online.

## 14.9 My Certificate Details

Click **CERTIFICATES > My Certificates** to open the **My Certificates** screen ([Figure 102 on page 172](#)). Click the details button to open the **My Certificate Details** screen. You can use this screen to view in-depth certificate information and change the certificate's name. In the case of a self-signed certificate, you can set it to be the one that the ZyXEL Device uses to sign the trusted remote host certificates that you import to the ZyXEL Device.

**Figure 105** My Certificate Details

|  |  |
|--|--|
| <b>Name</b>  | auto_generated_self_signed_cert  |
| <b>Property</b>  | <input checked="" type="checkbox"/> Default self-signed certificate which signs the imported remote host certificates. |
| <b>Certificate Path</b>  |  |
| <div>Searching...</div> <div>Refresh</div>   |  |
| <b>Certificate Information</b>   |  |
| <b>Type</b>  | Self-signed X.509 Certificate  |
| <b>Version</b>   | V3   |
| <b>Serial Number</b>   | 946685120  |
| <b>Subject</b>   | CN=NWA-3160 0019CB000001   |
| <b>Issuer</b>  | CN=NWA-3160 0019CB000001   |
| <b>Signature Algorithm</b>   | rsa-pkcs1-sha1   |
| <b>Valid From</b>  | 2000 Jan 1st, 00:00:00 GMT   |
| <b>Valid To</b>  | 2030 Jan 1st, 00:00:00 GMT   |
| <b>Key Algorithm</b>   | rsaEncryption (512 bits)   |
| <b>Subject Alternative Name</b>  | EMAIL=0019CB000001@auto.gen.cert   |
| <b>Key Usage</b>   | DigitalSignature, KeyEncipherment, KeyCertSign   |
| <b>Basic Constraint</b>  | Subject Type=CA, Path Length Constraint=1  |
| <b>MD5 Fingerprint</b>   | 2b:d5:da:d5:cf:ae:b7:96:06:72:c2:24:0c:49:e0:2d  |
| <b>SHA1 Fingerprint</b>  | af:f6:db:ac:fe:ab:13:d1:43:24:bf:4f:43:e2:4d:4f:d7:f2:18:aa  |
| <b>Certificate in PEM (Base-64) Encoded Format</b>   |  |
| <pre> eUFJU1BHLTEwMDBQIEZhY3RvcnkgRGVmYXVsdCBDZXJOaWZpY2F0ZTAeFwOwMDAx MDEwMDAwMDBaFw0zMDEwMDEwMDAwMDBaMDQxMjAwBgNVBAMTKVp5SQU1SIEctMTAw MFAgRmFjdG9yeSBEZSWZhdWx0IENlcnRpZml1YXRlMFwwDQYJKoZIhvcNAQEBBQAD SwAwSAJBANB1YebOCBx9tjUjVL2VoIFv1WBrQM613TF1WQoHKQtSFywWdFNnXXSL qXEX1YHfgoO6MnC6cJGUGGhd5pWau8MCaWEAAAN7MHkwDgYDVROPAQEABAQDAgKk MCAGA1UdEQQZMBeBFwZzhY3RvcnclAYXV0by5nZW4uY2YyY2VydDAsBgNVHRMBAQAECDAG AQH/AgEBMDEGA1UdJQQqMCgGCCsGAQUFCAICBggrBgEFBQcDAQYIKwYBBQUHAAwQG CCsGAQUFBwMCAOGCSqGSIb3DQEBBQUAAOEAk/6Za1/UjL+WZkiE+h6UmGJYT/gG D0yeDwtMQzydO2Rn3dLGI9QJtZwJrD8njPGv3oR7A2rcw1T2VQkA9FA9g== -----END CERTIFICATE----- </pre> |  |
| <div>Export</div> <div>Apply</div> <div>Cancel</div>   |  |

The following table describes the labels in this screen.

### Table 59 My Certificate Details

| Label  | Description  |
|--|--|
| Name   | This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).   |
| Property<br>Default self-signed certificate which signs the imported remote host certificates. | <p>Select this check box to have the ZyXEL Device use this certificate to sign the trusted remote host certificates that you import to the ZyXEL Device. This check box is only available with self-signed certificates.</p> <p>If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.</p> |

**Table 59** My Certificate Details (continued)

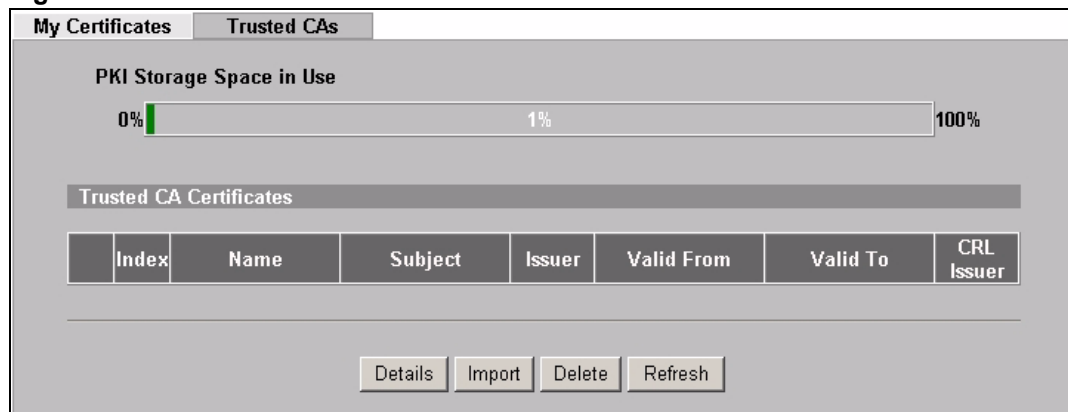
| LABEL                    | DESCRIPTION  |
|--------------------------|--|
| Certificate Path         | Click the <b>Refresh</b> button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself).<br>If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The ZyXEL Device does not trust the certificate and displays “Not trusted” in this field if any certificate on the path has expired or been revoked. |
| Refresh                  | Click <b>Refresh</b> to display the certification path.  |
| Certificate Information  | These read-only fields display detailed information about the certificate.   |
| Type                     | This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate’s owner signed the certificate (not a certification authority). “X.509” means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.  |
| Version                  | This field displays the X.509 version number.  |
| Serial Number            | This field displays the certificate’s identification number given by the certification authority or generated by the ZyXEL Device.   |
| Subject                  | This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).  |
| Issuer                   | This field displays identifying information about the certificate’s issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.<br>With self-signed certificates, this is the same as the <b>Subject Name</b> field.  |
| Signature Algorithm      | This field displays the type of algorithm that was used to sign the certificate. The ZyXEL Device uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use ras-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).  |
| Valid From               | This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.   |
| Valid To                 | This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.  |
| Key Algorithm            | This field displays the type of algorithm that was used to generate the certificate’s key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).   |
| Subject Alternative Name | This field displays the certificate owner’s IP address (IP), domain name (DNS) or e-mail address (EMAIL).  |
| Key Usage                | This field displays for what functions the certificate’s key can be used. For example, “DigitalSignature” means that the key can be used to sign certificates and “KeyEncipherment” means that the key can be used to encrypt text.  |
| Basic Constraint         | This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority’s certificate and “Path Length Constraint=1” means that there can only be one certification authority in the certificate’s path.  |
| MD5 Fingerprint          | This is the certificate’s message digest that the ZyXEL Device calculated using the MD5 algorithm.   |

**Table 59** My Certificate Details (continued)

| LABEL                                       | DESCRIPTION  |
|---|--|
| SHA1 Fingerprint                            | This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm.  |
| Certificate in PEM (Base-64) Encoded Format | <p>This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.</p> <p>You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment.</p> <p>You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p> |
| Export                                      | Click this button and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .  |
| Apply                                       | Click <b>Apply</b> to save your changes. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.   |
| Cancel                                      | Click <b>Cancel</b> to quit and return to the <b>My Certificates</b> screen.   |

## 14.10 Trusted CAs

Click **CERTIFICATES > Trusted CAs** to open the **Trusted CAs** screen. This screen displays a summary list of certificates of the certification authorities that you have set the ZyXEL Device to accept as trusted. The ZyXEL Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities. See the following figure.

**Figure 106** Trusted CAs

The following table describes the labels in this screen.

**Table 60** Trusted CAs

| LABEL                    | DESCRIPTION   |
|--------------------------|---|
| PKI Storage Space in Use | This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.   |
| Index                    | This field displays the certificate index number. The certificates are listed in alphabetical order.  |
| Name                     | This field displays the name used to identify this certificate.   |
| Subject                  | This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.  |
| Issuer                   | This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the <b>Subject</b> field.   |
| Valid From               | This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.  |
| Valid To                 | This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.   |
| CRL Issuer               | This field displays Yes if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the <b>Issues certificate revocation lists (CRL)</b> check box in the certificate's details screen to have the ZyXEL Device check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays "No". |
| Details                  | Click <b>Details</b> to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyXEL Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.  |
| Import                   | Click <b>Import</b> to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyXEL Device.  |
| Delete                   | Click <b>Delete</b> to delete an existing certificate. A window display asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.  |
| Refresh                  | Click this button to display the current validity status of the certificates.   |

## 14.11 Importing a Trusted CA's Certificate

Click **CERTIFICATES > Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate to the ZyXEL Device, see the following figure.



You must remove any spaces from the certificate's filename before you can import the certificate.

**Figure 107** Trusted CA Import

The following table describes the labels in this screen.

**Table 61** Trusted CA Import

| LABEL     | DESCRIPTION  |
|-----------|--|
| File Path | Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it. |
| Browse    | Click <b>Browse</b> to find the certificate file you want to upload.                                 |
| Apply     | Click <b>Apply</b> to save the certificate on the ZyXEL Device.                                      |
| Cancel    | Click <b>Cancel</b> to quit and return to the <b>Trusted CAs</b> screen.                             |

## 14.12 Trusted CA Certificate Details

Click **CERTIFICATES > Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen. Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyXEL Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

**Figure 108** Trusted CA Details

**Name:** VeriSign.cer

**Property**  
☐ Check incoming certificates issued by this CA against a CRL

**Certificate Path**

Searching...

Refresh

**Certificate Information**

**Type** Self-signed X.509 Certificate  
**Version** V1  
**Serial Number** 3558802160848854062232407011527417280  
**Subject** OU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US  
**Issuer** OU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US  
**Signature Algorithm** rsa-pkcs1-md2  
**Valid From** 1994 Nov 9th, 00:00:00 GMT  
**Valid To** 2010 Jan 7th, 23:59:59 GMT  
**Key Algorithm** rsaEncryption (1000 bits)  
**MD5 Fingerprint** 74:7b:82:03:43:00:00:9e:6b:b3:ec:47:bf:85:a5:93  
**SHA1 Fingerprint** 44:63:c5:31:d7:cc:c1:00:67:94:61:2b:b6:56:d3:bf:82:57:84:6f

**Certificate in PEM (Base-64) Encoded Format**

```
-----BEGIN CERTIFICATE-----
MIICNDCCAaECEAKtZn5ORf5eV288mBle3cAwDQYJKoZIhvcNAQECBQAwXzELMAkG
A1UEBhMCVVMxIDAeBgNVBAAwTF1JTQSBYXRhIFN1Y3VyaXR5LCBJbmMuMS4wLAYD
VQOLEyVTZW1cmUgU2VydGVyIEN1cnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTEkO
MTEwOTAuMDAwMFoXDTEwMDEwNzIzNTkxOVowXzELMAkGA1UEBhMCVVMxIDAeBgNV
BAAwTF1JTQSBYXRhIFN1Y3VyaXR5LCBJbmMuMS4wLAYDVQOLEyVTZW1cmUgU2Vy
dmV5IEN1cnRpZmljYXRpb24gQXV0aG9yaXR5MIGbMA0GCsgGSIB3DQEBAAQUAA4GJ
ADCBhQJ+AJLOesGugz5aqomDV6w1AXYMrca6OLDf06zV4ZFQD5YR&Ucm/jwjii0II
OhaGN1XpsSECrXZogZoFokvJ5yVmI1ZsiAeP94FZbYQHZZATcXY+m3dM41CJVphI
uR2nKR0TLkoRWZweFdVJVCxzCmmCsZc5nG1w20j13S3WyB57AgMBAAEwDQYJKoZI

```

Export Apply Cancel

The following table describes the labels in this screen.

**Table 62** Trusted CA Details

| LABEL  | DESCRIPTION  |
|--|--|
| Name   | This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).   |
| Property<br>Check incoming<br>certificates issued<br>by this CA against a<br>CRL | Select this check box to have the ZyXEL Device check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).<br>Clear this check box to have the ZyXEL Device not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).  |
| Certificate Path   | Click the <b>Refresh</b> button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the end entity's own certificate). The ZyXEL Device does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked. |
| Refresh  | Click <b>Refresh</b> to display the certification path.  |

**Table 62** Trusted CA Details (continued)

| LABEL                    | DESCRIPTION   |
|--------------------------|---|
| Certificate Information  | These read-only fields display detailed information about the certificate.  |
| Type                     | This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.   |
| Version                  | This field displays the X.509 version number.   |
| Serial Number            | This field displays the certificate's identification number given by the certification authority.   |
| Subject                  | This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).   |
| Issuer                   | This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.<br>With self-signed certificates, this is the same information as in the <b>Subject Name</b> field.  |
| Signature Algorithm      | This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use ras-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).   |
| Valid From               | This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.  |
| Valid To                 | This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.   |
| Key Algorithm            | This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyXEL Device uses RSA encryption) and the length of the key set in bits (1024 bits for example).  |
| Subject Alternative Name | This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).   |
| Key Usage                | This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.   |
| Basic Constraint         | This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.   |
| CRL Distribution Points  | This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.  |
| MD5 Fingerprint          | This is the certificate's message digest that the ZyXEL Device calculated using the MD5 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the ZyXEL Device has signed the certificate; thus causing this value to be different from that of the remote host's actual certificate. See <a href="#">Section 14.3 on page 170</a> for how to verify a remote host's certificate before you import it into the ZyXEL Device. |

**Table 62** Trusted CA Details (continued)

| LABEL                                       | DESCRIPTION  |
|---|--|
| SHA1 Fingerprint                            | This is the certificate's message digest that the ZyXEL Device calculated using the SHA1 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the ZyXEL Device has signed the certificate; thus causing this value to be different from that of the remote host's actual certificate. See <a href="#">Section 14.3 on page 170</a> for how to verify a remote host's certificate before you import it into the ZyXEL Device. |
| Certificate in PEM (Base-64) Encoded Format | This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.<br><br>You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).               |
| Export                                      | Click this button and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .  |
| Apply                                       | Click <b>Apply</b> to save your changes. You can only change the name and/or set whether or not you want the ZyXEL Device to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority.  |
| Cancel                                      | Click <b>Cancel</b> to quit and return to the <b>Trusted CAs</b> screen.   |



# Log Screens

This chapter contains information about configuring general log settings and viewing the ZyXEL Device's logs.

## 15.1 Configuring View Log

The web configurator allows you to look at all of the ZyXEL Device's logs in one location.

Click **LOGS > View Log**. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see [Figure 110 on page 189](#)). Options include logs about system maintenance, system errors and access control.

You can view logs and alert messages in this page. Once the log entries are all used, the log will wrap around and the old logs will be deleted.

Click a column heading to sort the entries. A triangle indicates the direction of the sort order.

**Figure 109** View Log

| View Log |                        | Log Settings                             |               |             |   |
|----------|------------------------|--|---------------|-------------|---|
| Display  |                        | All Logs                                 | Email Log Now | Refresh     | Clear Log   |
| Index    | Time ▲                 | Message                                  | Source        | Destination | Notes   |
| 1        | 01/01/2000<br>21:34:51 | Rogue AP Detection.                      |               |             | MAC:00:13:a6:10:1b:c1,<br>Channel:01, Security:None,<br>SSID:testonly |
| 2        | 01/01/2000<br>21:24:24 | Cert trusted: CN=NWA3550<br>001349000001 |               |             | CERT MANAGER  |
| 3        | 01/01/2000<br>20:37:24 | Successful HTTPS login                   | 192.168.1.33  |             | User:admin  |

The following table describes the labels in this screen.

**Table 63** View Log

| LABEL   | DESCRIPTION  |
|---------|--|
| Display | Select a log category from the drop down list box to display logs within the selected category. To view all logs, select <b>All Logs</b> .<br>The number of categories shown in the drop down list box depends on the selection in the <b>Log Settings</b> page. |
| Time    | This field displays the time the log was recorded.   |
| Message | This field states the reason for the log.  |

**Table 63** View Log

| LABEL         | DESCRIPTION  |
|---------------|--|
| Source        | This field lists the source IP address and the port number of the incoming packet.                                 |
| Destination   | This field lists the destination IP address and the port number of the incoming packet.                            |
| Notes         | This field displays additional information about the log entry.  |
| Email Log Now | Click <b>Email Log Now</b> to send the log screen to the e-mail address specified in the <b>Log Settings</b> page. |
| Refresh       | Click <b>Refresh</b> to renew the log screen.  |
| Clear Log     | Click <b>Clear Log</b> to clear all the logs.  |

## 15.2 Configuring Log Settings

To change your ZyXEL Device's log settings, click **LOGS > Log Settings**. The screen appears as shown.

Use the **Log Settings** screen to configure to where and when the ZyXEL Device is to send the logs and which logs and/or immediate alerts it is to send.

An alert is a type of log that warrants more serious attention. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts are displayed in red and logs are displayed in black.

**Figure 110** Log Settings

The following table describes the labels in this screen.

**Table 64** Log Settings

| LABEL          | DESCRIPTION  |
|----------------|--|
| Address Info   |  |
| Mail Server    | Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail. |
| Mail Subject   | Type a title that you want to be in the subject line of the log e-mail message that the ZyXEL Device sends.  |
| Send Log to    | Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.  |
| Send Alerts to | Enter the e-mail address where the alert messages will be sent. If this field is left blank, alert messages will not be sent via e-mail.   |

**Table 64** Log Settings

| LABEL                        | DESCRIPTION  |
|------------------------------|--|
| SMTP Authentication          | If you use SMTP authentication, the mail receiver should be the owner of the SMTP account.   |
| User Name                    | If your e-mail account requires SMTP authentication, enter the username here.  |
| Password                     | Enter the password associated with the above username.   |
| Syslog Logging               | Syslog logging sends a log to an external syslog server used to store logs.  |
| Active                       | Click <b>Active</b> to enable syslog logging.  |
| Syslog IP Address            | Enter the server name or IP address of the syslog server that will log the selected categories of logs.  |
| Log Facility                 | Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.  |
| Send Log                     |  |
| Log Schedule                 | <p>This drop-down menu is used to configure the frequency of log messages being sent as E-mail:</p> <ul style="list-style-type: none"> <li>• Daily</li> <li>• Weekly</li> <li>• Hourly</li> <li>• When Log is Full</li> <li>• None.</li> </ul> <p>If the <b>Weekly</b> or the <b>Daily</b> option is selected, specify a time of day when the E-mail should be sent. If the <b>Weekly</b> option is selected, then also specify which day of the week the E-mail should be sent. If the <b>When Log is Full</b> option is selected, an alert is sent when the log fills up. If you select <b>None</b>, no log messages are sent.</p> |
| Day for Sending Log          | This field is only available when you select <b>Weekly</b> in the <b>Log Schedule</b> field. Use the drop down list box to select which day of the week to send the logs.  |
| Time for Sending Log         | Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.  |
| Clear log after sending mail | Select the check box to clear all logs after logs and alert messages are sent via e-mail.  |
| Log                          | Select the categories of logs that you want to record.   |
| Send Immediate Alert         | Select the categories of alerts for which you want the ZyXEL Device to immediately send e-mail alerts.   |
| Apply                        | Click <b>Apply</b> to save your customized settings and exit this screen.  |
| Reset                        | Click <b>Reset</b> to reconfigure all the fields in this screen.   |

## 15.3 Example Log Messages

This section provides descriptions of some example log messages.

**Table 65** System Maintenance Logs

| LOG MESSAGE                    | DESCRIPTION   |
|--------------------------------|---|
| Time calibration is successful | The router has adjusted its time based on information from the time server. |
| Time calibration failed        | The router failed to get information from the time server.                  |

**Table 65** System Maintenance Logs

| LOG MESSAGE               | DESCRIPTION  |
|---------------------------|--|
| DHCP client gets %s       | A DHCP client got a new IP address from the DHCP server.                 |
| DHCP client IP expired    | A DHCP client's IP address has expired.                                  |
| DHCP server assigns %s    | The DHCP server assigned an IP address to a client.                      |
| SMT Login Successfully    | Someone has logged on to the router's SMT interface.                     |
| SMT Login Fail            | Someone has failed to log on to the router's SMT interface.              |
| WEB Login Successfully    | Someone has logged on to the router's web configurator interface.        |
| WEB Login Fail            | Someone has failed to log on to the router's web configurator interface. |
| TELNET Login Successfully | Someone has logged on to the router via telnet.                          |
| TELNET Login Fail         | Someone has failed to log on to the router via telnet.                   |
| FTP Login Successfully    | Someone has logged on to the router via FTP.                             |
| FTP Login Fail            | Someone has failed to log on to the router via FTP.                      |

**Table 66** ICMP Notes

| TYPE | CODE | DESCRIPTION   |
|------|------|---|
| 0    |      | Echo Reply  |
|      | 0    | Echo reply message  |
| 3    |      | Destination Unreachable   |
|      | 0    | Net unreachable   |
|      | 1    | Host unreachable  |
|      | 2    | Protocol unreachable  |
|      | 3    | Port unreachable  |
|      | 4    | A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)  |
|      | 5    | Source route failed   |
| 4    |      | Source Quench   |
|      | 0    | A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network. |
| 5    |      | Redirect  |
|      | 0    | Redirect datagrams for the Network  |
|      | 1    | Redirect datagrams for the Host   |
|      | 2    | Redirect datagrams for the Type of Service and Network  |
|      | 3    | Redirect datagrams for the Type of Service and Host   |
| 8    |      | Echo  |
|      | 0    | Echo message  |
| 11   |      | Time Exceeded   |
|      | 0    | Time to live exceeded in transit  |
|      | 1    | Fragment reassembly time exceeded   |
| 12   |      | Parameter Problem   |

**Table 66** ICMP Notes (continued)

| TYPE | CODE | DESCRIPTION                 |
|------|------|-----------------------------|
|      | 0    | Pointer indicates the error |
| 13   |      | Timestamp                   |
|      | 0    | Timestamp request message   |
| 14   |      | Timestamp Reply             |
|      | 0    | Timestamp reply message     |
| 15   |      | Information Request         |
|      | 0    | Information request message |
| 16   |      | Information Reply           |
|      | 0    | Information reply message   |

**Table 67** Sys log

| LOG MESSAGE   | DESCRIPTION  |
|---|--|
| Mon dd hr:mm:ss hostname<br>src=<srcIP:srcPort><br>dst=<dstIP:dstPort><br>msg=<msg> note=<note> | This message is sent by the "RAS" when this syslog is generated. The messages and notes are defined in this appendix's other charts. |

## 15.4 Log Commands

Go to the command interpreter interface (see [Chapter 24 on page 249](#) for how to access and use the commands).

### 15.4.1 Configuring What You Want the ZyXEL Device to Log

Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the ZyXEL Device is to record.

Use `sys logs category` followed by a log category and a parameter to decide what to record

**Table 68** Log Categories and Available Settings Example

| LOG CATEGORIES  | AVAILABLE PARAMETERS |
|---|----------------------|
| error   | 0, 1, 2, 3           |
| mten  | 0, 1                 |
| Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category. |                      |

Use the `sys logs save` command to store the settings in the ZyXEL Device (you must do this in order to record logs).

### 15.4.2 Displaying Logs

Use the `sys logs display` command to show all of the logs in the ZyXEL Device's log.

Use the `sys logs category display` command to show the log settings for all of the log categories.

Use the `sys logs display [log category]` command to show the logs in an individual ZyXEL Device log category.

Use the `sys logs clear` command to erase all of the ZyXEL Device's logs.

## 15.5 Log Command Example

This example shows how to set the ZyXEL Device to record the error logs and alerts and then view the results.

```
ras> sys logs load
ras> sys logs category error 3
ras> sys logs save
ras> sys logs display access
```

| #. | time                | source          | destination        | notes  | message |
|----|---------------------|-----------------|--------------------|--------|---------|
| 0  | 11/11/2002 15:10:12 | 172.22.3.80:137 | 172.22.255.255:137 | ACCESS | BLOCK   |



This chapter discusses how to configure VLAN on the ZyXEL Device.

## 16.1 VLAN

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network can belong to one or more groups. Only stations within the same group can talk to each other.

### 16.1.1 Management VLAN ID

The Management VLAN ID identifies the “management VLAN”. A device must be a member of this “management VLAN” in order to access and manage the ZyXEL Device. If a device is not a member of this VLAN, then that device cannot manage the ZyXEL Device.



---

If no devices are in the management VLAN, then you will be able to access the ZyXEL Device only through the console port (not through the network).

---

### 16.1.2 VLAN Tagging

The ZyXEL Device supports IEEE 802.1q VLAN tagging. Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header of a frame to identify VLAN membership. The ZyXEL Device can identify VLAN tags for incoming Ethernet frames and add VLAN tags to outgoing Ethernet frames.



---

You must connect the ZyXEL Device to a VLAN-aware device that is a member of the management VLAN in order to perform management. See the [Configuring Management VLAN Example](#) BEFORE you configure the VLAN screens.

---

## 16.2 Configuring VLAN

The ZyXEL Device allows you to configure VLAN based on SSID profile (wireless VLAN), and / or based on your RADIUS server (RADIUS VLAN).

- When you use wireless VLAN, the ZyXEL Device tags all packets from an SSID with the VLAN ID you set in the **Wireless VLAN** screen.
- When you use RADIUS VLAN, your RADIUS server assigns VLAN IDs to a user or user group's traffic based on the configuration in the **RADIUS VLAN** screen.
- When you use wireless VLAN and RADIUS VLAN together, the ZyXEL Device first tries to assign VLAN IDs based on RADIUS VLAN configuration. If a client's user name does not match an entry in the **RADIUS VLAN** screen, the ZyXEL Device assigns a VLAN ID based on the settings in the **Wireless VLAN** screen. See [Section 16.2.4 on page 202](#) for more information.



---

To use RADIUS VLAN, you must first select **Enable VIRTUAL LAN** and configure the **Management VLAN ID** in the **VLAN > Wireless VLAN** screen.

---

### 16.2.1 Wireless VLAN

Click **VLAN > Wireless VLAN**. The following screen appears.

**Figure 111** Wireless VLAN

Wireless VLAN
RADIUS VLAN

VIRTUAL LAN Setup

☒ Enable VIRTUAL LAN

Wireless VIRTUAL LAN Setup

Management VLAN ID
 (1 ~ 4094)

VLAN Mapping Table

| Index | Name       | SSID    | VLAN ID                         | Second Rx VLAN ID              |
|-------|------------|---------|---------------------------------|--------------------------------|
| 1     | VoIP_SSID  | ZyXEL01 | <input type="text" value="1"/>  | <input type="text" value="0"/> |
| 2     | Guest_SSID | ZyXEL02 | <input type="text" value="2"/>  | <input type="text" value="0"/> |
| 3     | SSID03     | ZyXEL03 | <input type="text" value="3"/>  | <input type="text" value="0"/> |
| 4     | SSID04     | ZyXEL04 | <input type="text" value="4"/>  | <input type="text" value="0"/> |
| 5     | SSID05     | ZyXEL05 | <input type="text" value="5"/>  | <input type="text" value="0"/> |
| 6     | SSID06     | ZyXEL06 | <input type="text" value="6"/>  | <input type="text" value="0"/> |
| 7     | SSID07     | ZyXEL07 | <input type="text" value="7"/>  | <input type="text" value="0"/> |
| 8     | SSID08     | ZyXEL08 | <input type="text" value="8"/>  | <input type="text" value="0"/> |
| 9     | SSID09     | ZyXEL09 | <input type="text" value="9"/>  | <input type="text" value="0"/> |
| 10    | SSID10     | ZyXEL10 | <input type="text" value="10"/> | <input type="text" value="0"/> |
| 11    | SSID11     | ZyXEL11 | <input type="text" value="11"/> | <input type="text" value="0"/> |
| 12    | SSID12     | ZyXEL12 | <input type="text" value="12"/> | <input type="text" value="0"/> |
| 13    | SSID13     | ZyXEL13 | <input type="text" value="13"/> | <input type="text" value="0"/> |
| 14    | SSID14     | ZyXEL14 | <input type="text" value="14"/> | <input type="text" value="0"/> |
| 15    | SSID15     | ZyXEL15 | <input type="text" value="15"/> | <input type="text" value="0"/> |
| 16    | SSID16     | ZyXEL16 | <input type="text" value="16"/> | <input type="text" value="0"/> |

The following table describes the labels in this screen

**Table 69** Wireless VLAN

| FIELD              | DESCRIPTION   |
|--------------------|---|
| Enable VIRTUAL LAN | Select this box to enable VLAN tagging.   |
| Management VLAN ID | <p>Enter a number from 1 to 4094 to define this VLAN group. At least one device in your network must belong to this VLAN group in order to manage the ZyXEL Device.</p> <p>Note: Mail and FTP servers must have the same management VLAN ID to communicate with the ZyXEL Device.</p> <p>See <a href="#">Section 16.2.3 on page 199</a> for more information.</p> |
| VLAN Mapping Table | Use this table to have the ZyXEL Device assign VLAN tags to packets from wireless clients based on the SSID they use to connect to the ZyXEL Device.  |
| Index              | This is the index number of the SSID profile.   |

**Table 69** Wireless VLAN

| FIELD             | DESCRIPTION  |
|-------------------|--|
| Name              | This is the name of the SSID profile.  |
| SSID              | This is the SSID the profile uses.   |
| VLAN ID           | Enter a VLAN ID number from 1 to 4094. Packets coming from the WLAN using this SSID profile are tagged with the VLAN ID number by the ZyXEL Device. Different SSID profiles can use the same or different VLAN IDs. This allows you to split wireless stations into groups using similar VLAN IDs.                             |
| Second Rx VLAN ID | Enter a number from 1 to 4094, but different from the entry's <b>VLAN ID</b> . Traffic received from the LAN that is tagged with this VLAN ID is sent to all SSIDs with this VLAN ID configured in the <b>VLAN ID</b> or <b>Second Rx VLAN ID</b> fields. See <a href="#">Section 16.2.5 on page 210</a> for more information. |
| Apply             | Click this to save your changes to the ZyXEL Device.   |
| Reset             | Click this to return this screen to its last-saved settings.   |

## 16.2.2 RADIUS VLAN

Click **VLAN > RADIUS VLAN**. The following screen appears.

**Figure 112** RADIUS VLAN

**Wireless VLAN**   **RADIUS VLAN**

**RADIUS VIRTUAL LAN Setup**

☐ Block station if RADIUS server assigns VLAN name error.

**VLAN Mapping Table**

| Index | Active                   | VLAN ID | Name  |
|-------|--------------------------|---------|-------|
| 1     | <input type="checkbox"/> | 1       | zyxel |
| 2     | <input type="checkbox"/> | 1       | zyxel |
| 3     | <input type="checkbox"/> | 1       | zyxel |
| 4     | <input type="checkbox"/> | 1       | zyxel |
| 5     | <input type="checkbox"/> | 1       | zyxel |
| 6     | <input type="checkbox"/> | 1       | zyxel |
| 7     | <input type="checkbox"/> | 1       | zyxel |
| 8     | <input type="checkbox"/> | 1       | zyxel |
| 9     | <input type="checkbox"/> | 1       | zyxel |
| 10    | <input type="checkbox"/> | 1       | zyxel |
| 11    | <input type="checkbox"/> | 1       | zyxel |
| 12    | <input type="checkbox"/> | 1       | zyxel |
| 13    | <input type="checkbox"/> | 1       | zyxel |
| 14    | <input type="checkbox"/> | 1       | zyxel |
| 15    | <input type="checkbox"/> | 1       | zyxel |
| 16    | <input type="checkbox"/> | 1       | zyxel |

Apply   Reset

The following table describes the labels in this screen.

**Table 70** RADIUS VLAN

| LABEL   | DESCRIPTION   |
|---|---|
| Block station if RADIUS server assigns VLAN name error! | Select this to have the ZyXEL Device forbid access to wireless clients when the VLAN attributes sent from the RADIUS server do not match a configured <b>Name</b> field.<br>When you select this check box, only users with names configured in this screen can access the network through the ZyXEL Device.  |
| VLAN Mapping Table                                      | Use this table to map names to VLAN IDs so that the RADIUS server can assign each user or user group a mapped VLAN ID. See your RADIUS server documentation for more information on configuring VLAN ID attributes.<br>See <a href="#">Section 16.2.4 on page 202</a> for more information.   |
| Index   | This is the index number of the VLAN mapping profile.   |
| Active  | Select a check box to enable the VLAN mapping profile.  |
| VLAN ID   | Type a VLAN ID. Incoming traffic from the WLAN is authorized and assigned a VLAN ID before it is sent to the LAN.   |
| Name  | Type a name to have the ZyXEL Device check for specific VLAN attributes on incoming messages from the RADIUS server. Access-accept packets sent by the RADIUS server contain VLAN related attributes. The configured <b>Name</b> fields are checked against these attributes. If a configured <b>Name</b> field matches these attributes, the corresponding VLAN ID is added to packets sent from this user to the LAN.<br><br>If the VLAN-related attributes sent by the RADIUS server do not match a configured <b>Name</b> field, a wireless station is assigned the wireless VLAN ID associated with its SSID (unless the <b>Block station if RADIUS server assigns VLAN error!</b> check box is selected). |
| Apply   | Click <b>Apply</b> to save your changes to the ZyXEL Device.  |
| Reset   | Click <b>Reset</b> to begin configuring this screen afresh.   |

### 16.2.3 Configuring Management VLAN Example

This section shows you how to create a VLAN on an Ethernet switch.

By default, the port on the ZyXEL Device is a member of the management VLAN (VLAN ID 1). The following procedure shows you how to configure a tagged VLAN.

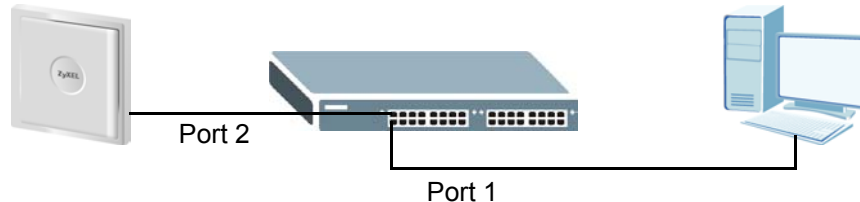


Use the out-of-band management port or console port to configure the switch if you misconfigure the management VLAN and lock yourself out from performing in-band management.

On an Ethernet switch, create a VLAN that has the same management VLAN ID as the ZyXEL Device. The following figure has the ZyXEL Device connected to port 2 of the switch and your computer connected to port 1. The management VLAN ID is ten.

**Figure 113** Management VLAN Configuration Example

MVID = 10



Perform the following steps in the switch web configurator. This example uses the ZyXEL switch screenshots.

- 1 Click **VLAN** under **Advanced Application**.
- 2 Click **Static VLAN**.
- 3 Select the **ACTIVE** check box.
- 4 Type a **Name** for the VLAN ID.
- 5 Type a **VLAN Group ID**. This should be the same as the management VLAN ID on the ZyXEL Device.
- 6 Enable **Tx Tagging** on the port which you want to connect to the ZyXEL Device.  
Disable **Tx Tagging** on the port you are using to connect to your computer.
- 7 Under **Control**, select **Fixed** to set the ports (1 and 2 in this example) as a member of the VLAN.

**Figure 114** VLAN-Aware Switch - Static VLAN

The screenshot shows the 'Static VLAN' configuration interface. At the top, there's a 'Static VLAN' tab and a 'VLAN Status' link. The 'ACTIVE' checkbox is checked. The 'Name' field contains 'VID1' and the 'VLAN Group ID' field contains '10'. A red 'EXAMPLE' stamp is overlaid on the right. Below this, a table lists port configurations:

| Port | Control   | Tagging  |
|------|---|--|
| 1    | <input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden | <input type="checkbox"/> Tx Tagging            |
| 2    | <input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |

- 8 Click **Apply**. The following screen displays.

**Figure 115** VLAN-Aware Switch

The screenshot shows a table of configured VLANs. The first row is highlighted with a red box, indicating the example configuration. A red 'EXAMPLE' stamp is overlaid on the right side of the table.

| VID | Active | Name     | Delete                   |
|-----|--------|----------|--------------------------|
| 10  | Yes    | VID1     | <input type="checkbox"/> |
| 2   | Yes    | 2        | <input type="checkbox"/> |
| 3   | Yes    | 3        | <input type="checkbox"/> |
| 4   | Yes    | VLAN4    | <input type="checkbox"/> |
| 5   | Yes    | cth-test | <input type="checkbox"/> |

- 9 Click **VLAN Status** to display the following screen.

**Figure 116** VLAN-Aware Switch - VLAN Status

VLAN Status

VLAN Port Setting

Static VLAN

The Number Of VLAN = 5

| Index | VID | Port Number |   |   |   |    |    |    |    |    |    |    |    |    |    |   |   |   |   |   |   |   |   |   |   |   | Elapsed Time | Status |
|-------|-----|-------------|---|---|---|----|----|----|----|----|----|----|----|----|----|---|---|---|---|---|---|---|---|---|---|---|--------------|--------|
|       |     | 2           | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 | S2 |   |   |   |   |   |   |   |   |   |   |   |              |        |
| 1     | 10  | T           | - | - | - | T  | U  | -  | -  | -  | -  | -  | -  | -  | -  | - | - | - | - | - | - | - | - | - | - | - | 0:08:28      | Static |
|       |     | 1           | 3 | 5 | 7 | 9  | 11 | 13 | 15 | 17 | 19 | 21 | 23 | 25 | S1 |   |   |   |   |   |   |   |   |   |   |   |              |        |
|       |     | U           | - | - | - | -  | -  | -  | -  | -  | -  | -  | -  | -  | -  | - | - | - | - | - | - | - | - | - | - | - |              |        |
| 2     | 2   | T           | U | - | - | -  | -  | -  | -  | -  | -  | -  | -  | -  | -  | - | - | - | - | - | - | - | - | - | - | - | 0:08:28      | Static |
|       |     | -           | U | - | - | -  | -  | -  | -  | -  | -  | -  | -  | -  | -  | - | - | - | - | - | - | - | - | - | - | - |              |        |
|       |     | -           | - | - | - | -  | -  | -  | -  | -  | -  | -  | -  | -  | -  | - | - | - | - | - | - | - | - | - | - | - |              |        |
| 3     | 3   | T           | U | - | - | -  | -  | -  | -  | -  | -  | -  | -  | -  | -  | - | - | - | - | - | - | - | - | - | - | - | 0:08:28      | Static |
|       |     | -           | - | - | - | -  | -  | -  | -  | -  | -  | -  | -  | -  | -  | - | - | - | - | - | - | - | - | - | - | - |              |        |
|       |     | -           | - | - | - | -  | -  | -  | -  | -  | -  | -  | -  | -  | -  | - | - | - | - | - | - | - | - | - | - | - |              |        |
| 4     | 4   | -           | - | - | - | -  | -  | -  | -  | -  | -  | -  | -  | -  | -  | - | - | - | - | - | - | - | - | - | - | - | 0:08:27      | Static |
|       |     | -           | - | - | - | -  | -  | -  | -  | -  | -  | -  | -  | -  | -  | - | - | - | - | - | - | - | - | - | - | - |              |        |
|       |     | -           | - | - | - | -  | -  | -  | -  | -  | -  | -  | -  | -  | -  | - | - | - | - | - | - | - | - | - | - | - |              |        |
| 5     | 5   | -           | - | - | - | -  | -  | -  | -  | -  | -  | -  | -  | -  | -  | - | - | - | - | - | - | - | - | - | - | - | 0:08:27      | Static |
|       |     | -           | - | - | - | -  | -  | -  | -  | -  | -  | -  | -  | -  | -  | - | - | - | - | - | - | - | - | - | - | - |              |        |
|       |     | -           | - | - | - | -  | -  | -  | -  | -  | -  | -  | -  | -  | -  | - | - | - | - | - | - | - | - | - | - | - |              |        |

EXAMPLE

Follow the instructions in the Quick Start Guide to set up your ZyXEL Device for configuration. The ZyXEL Device should be connected to the VLAN-aware switch. In the above example, the switch is using port 1 to connect to your computer and port 2 to connect to the ZyXEL Device: [Figure 113 on page 200](#).

- 1 In the ZyXEL Device web configurator click **VLAN** to open the VLAN setup screen.
- 2 Select the **Enable VIRTUAL LAN** check box and type a **Management VLAN ID** (10 in this example) in the field provided.
- 3 Click **Apply**.

**Figure 117** VLAN Setup

**WIRELESS VLAN** **RADIUS VLAN**

**VIRTUAL LAN Setup**

☒ **Enable VIRTUAL LAN**

**Wireless VIRTUAL LAN Setup**

Management VLAN ID:  (1 ~ 4094)

**VLAN Mapping Table**

| Index | Name       | SSID    | VLAN ID | Second Rx VLAN ID |
|-------|------------|---------|---------|-------------------|
| 1     | VoIP_SSID  | ZyXEL01 | 1       | 0                 |
| 2     | Guest_SSID | ZyXEL02 | 2       | 0                 |
| 3     | SSID03     | ZyXEL03 | 3       | 0                 |
| 4     | SSID04     | ZyXEL04 | 4       | 0                 |
| 5     | SSID05     | ZyXEL05 | 5       | 0                 |
| 6     | SSID06     | ZyXEL06 | 6       | 0                 |
| 7     | SSID07     | ZyXEL07 | 7       | 0                 |
| 8     | SSID08     | ZyXEL08 | 8       | 0                 |
| 9     | SSID09     | ZyXEL09 | 9       | 0                 |
| 10    | SSID10     | ZyXEL10 | 10      | 0                 |
| 11    | SSID11     | ZyXEL11 | 11      | 0                 |
| 12    | SSID12     | ZyXEL12 | 12      | 0                 |
| 13    | SSID13     | ZyXEL13 | 13      | 0                 |
| 14    | SSID14     | ZyXEL14 | 14      | 0                 |
| 15    | SSID15     | ZyXEL15 | 15      | 0                 |
| 16    | SSID16     | ZyXEL16 | 16      | 0                 |

- 4 The ZyXEL Device attempts to connect with a VLAN-aware device. You can now access and manage the ZyXEL Device through the Ethernet switch.



If you do not connect the ZyXEL Device to a correctly configured VLAN-aware device, you will lock yourself out of the ZyXEL Device. If this happens, you must reset the ZyXEL Device to access it again.

## 16.2.4 Configuring Microsoft's IAS Server Example

Dynamic VLAN assignment can be used with the ZyXEL Device. Dynamic VLAN assignment allows network administrators to assign a specific VLAN (configured on the ZyXEL Device) to an individual's Windows User Account. When a wireless station is successfully authenticated to the network, it is automatically placed into its respective VLAN.

ZyXEL uses the following standard RADIUS attributes returned from Microsoft's IAS (Internet Authentication Service) RADIUS service to place the wireless station into the correct VLAN:

**Table 71** Standard RADIUS Attributes

| ATTRIBUTE NAME          | TYPE | VALUE   |
|-------------------------|------|---|
| Tunnel-Type             | 064  | 13 (decimal) – VLAN   |
| Tunnel-Medium-Type      | 065  | 6 (decimal) – 802   |
| Tunnel-Private-Group-ID | 081  | <vlan-name> (string) – either the <b>Name</b> you enter in the ZyXEL Device's <b>VLAN &gt; RADIUS VLAN</b> screen or the number. See <a href="#">Figure 129 on page 208</a> . |

The following occurs under Dynamic VLAN Assignment:

- 1 When you configure your wireless credentials, the ZyXEL Device sends the information to the IAS server using RADIUS protocol.
- 2 Authentication by the RADIUS server is successful.
- 3 The RADIUS server sends three attributes related to this feature.
- 4 The ZyXEL Device compares these attributes with the VLAN screen mapping table.
  - 4a If the **Name**, for example “VLAN 20” is found, the mapped VLAN ID is used.
  - 4b If the **Name** is not found in the mapping table, the string in the **Tunnel-Private-Group-ID** attribute is considered as a number ID format, for example 2493. The range of the number ID (Name:string) is between 1 and 4094.
  - 4c If **a** or **b** are not matched, the ZyXEL Device uses the VLAN ID configured in the **Wireless VLAN** screen and the wireless station. The **VLAN ID** in the **Wireless VLAN** screen is independent and hence different to the **VLAN ID** in the **RADIUS VLAN** screen.

### 16.2.4.1 Configuring VLAN Groups

To configure a VLAN group you must first define the VLAN Groups on the Active Directory server and assign the user accounts to each VLAN Group.

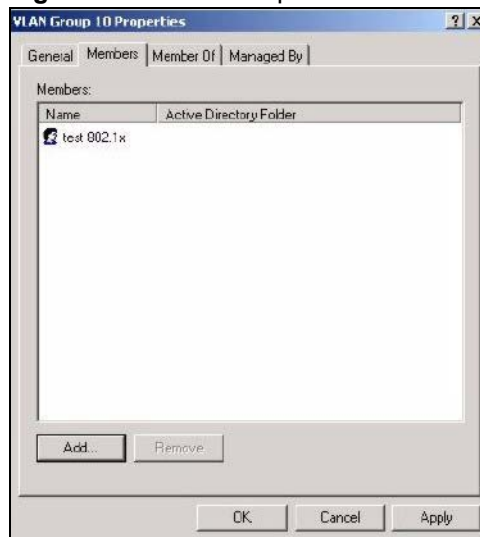
- 1 Using the Active Directory Users and Computers administrative tool, create the VLAN Groups that will be used for each VLAN ID. One VLAN Group must be created for each VLAN defined on the ZyXEL Device. The VLAN Groups must be created as **Global/Security** groups.
  - Type a name for the **VLAN Group** that describes the VLAN Group's function.
  - Select the **Global** Group scope parameter check box.
  - Select the **Security** Group type parameter check box.
  - Click **OK**.

**Figure 118** New Global Security Group

**2** In **VLAN Group ID Properties**, click the **Members** tab.

- The IAS uses group memberships to determine which user accounts belong to which VLAN groups. Click the **Add** button and configure the VLAN group details.

**3** Repeat the previous step to add each VLAN group required.

**Figure 119** Add Group Members

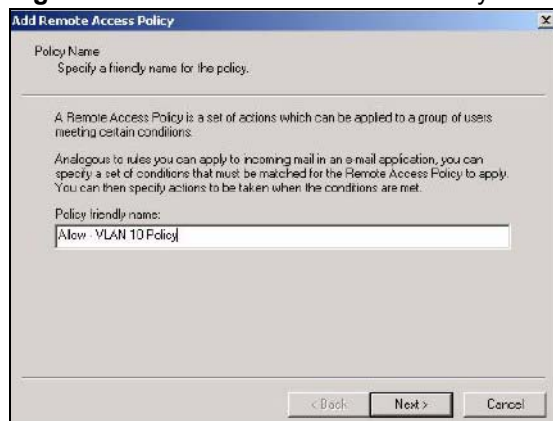
#### 16.2.4.2 Configuring Remote Access Policies

Once the VLAN Groups have been created, the IAS Remote Access Policy needs to be defined. This allows the IAS to compare the user account being authenticated against the group memberships of each VLAN Group.

- 1** Using the **Remote Access Policy** option on the Internet Authentication Service management interface, create a new VLAN Policy for each VLAN Group defined in the previous section. The order of the remote access policies is important. The most specific policies should be placed at the top of the policy list and the most general at the bottom. For example, if the Day-And-Time Restriction policy is still present, it should be moved to the bottom or deleted to allow the VLAN Group policies to take precedence.
- Right click **Remote Access Policy** and select **New Remote Access Policy**.

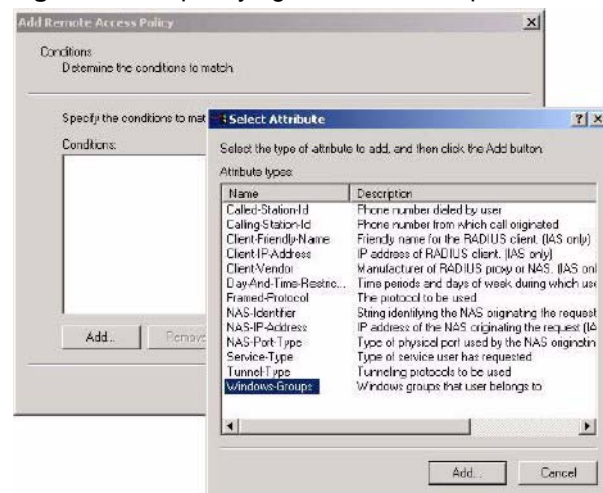
- Enter a **Policy friendly name** that describes the policy. Each Remote Access Policy will be matched to one VLAN Group. An example may be, **Allow - VLAN 10 Policy**.
- Click **Next**.

**Figure 120** New Remote Access Policy for VLAN Group

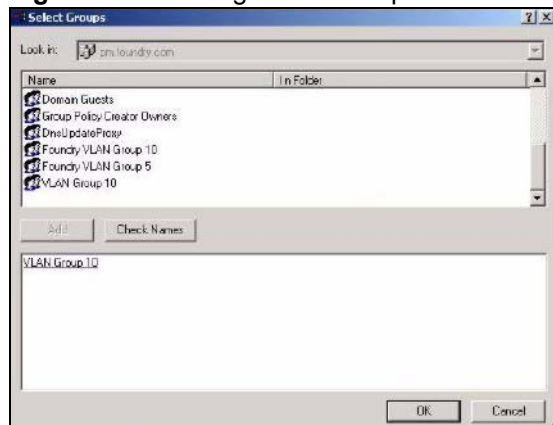


- 2 The **Conditions** window displays. Select **Add** to add a condition for this policy to act on.
- 3 In the **Select Attribute** screen, click **Windows-Groups** and the **Add** button.

**Figure 121** Specifying Windows-Group Condition

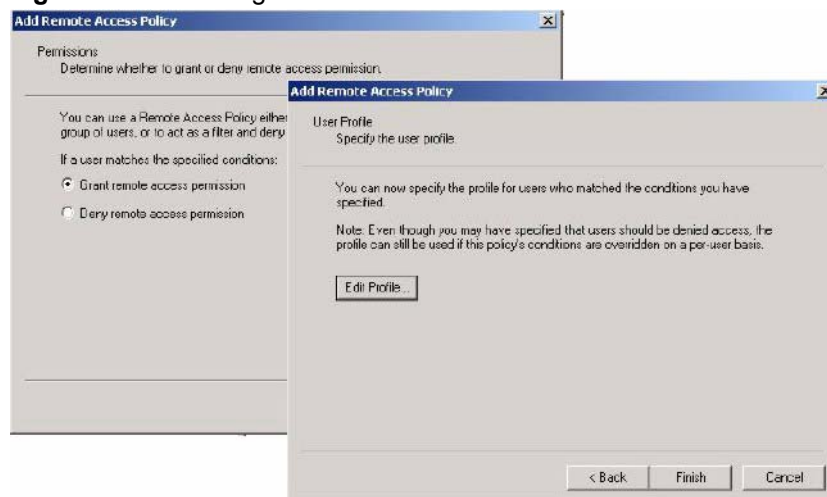


- 4 The **Select Groups** window displays. Select a remote access policy and click the **Add** button. The policy is added to the field below. Only one VLAN Group should be associated with each policy.
- 5 Click **OK** and **Next** in the next few screens to accept the group value.

**Figure 122** Adding VLAN Group

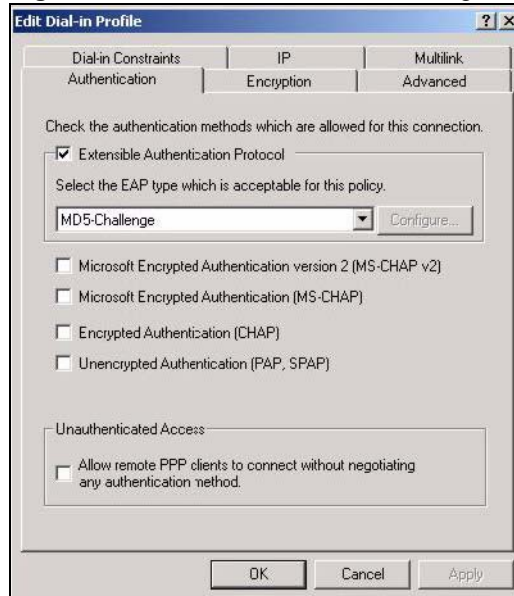
**6** When the **Permissions** options screen displays, select **Grant remote access permission**.

- Click **Next** to grant access based on group membership.
- Click the **Edit Profile** button.

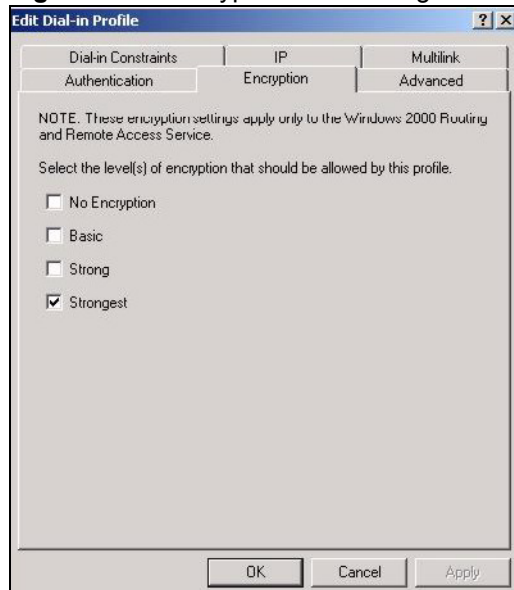
**Figure 123** Granting Permissions and User Profile Screens

**7** The **Edit Dial-in Profile** screen displays. Click the **Authentication** tab and select the **Extensible Authentication Protocol** check box.

- Select an EAP type depending on your authentication needs from the drop-down list box.
- Clear the check boxes for all other authentication types listed below the drop-down list box.

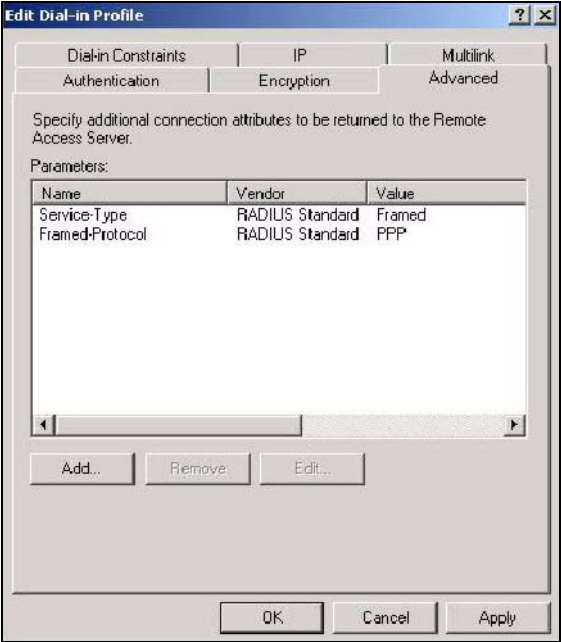
**Figure 124** Authentication Tab Settings

- 8** Click the **Encryption** tab. Select the **Strongest** encryption option. This step is not required for EAP-MD5, but is performed as a safeguard.

**Figure 125** Encryption Tab Settings

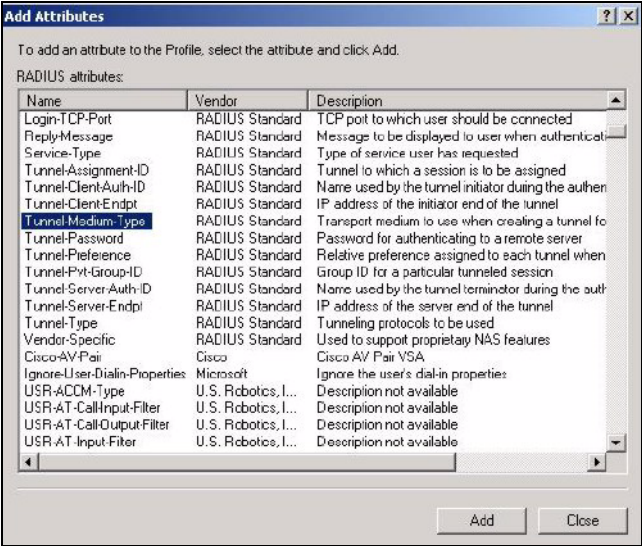
- 9** Click the **IP** tab and select the **Client may request an IP address** check box for DHCP support.
- 10** Click the **Advanced** tab. The current default parameters returned to the ZyXEL Device should be **Service-Type** and **Framed-Protocol**.
- Click the **Add** button to add an additional three RADIUS VLAN attributes required for 802.1X Dynamic VLAN Assignment.

Figure 126 Connection Attributes Screen



- 11 The RADIUS Attribute screen displays. From the list, three RADIUS attributes will be added:
- Tunnel-Medium-Type
  - Tunnel-Pvt-Group-ID
  - Tunnel-Type
- Click the **Add** button
  - Select **Tunnel-Medium-Type**
  - Click the **Add** button.

Figure 127 RADIUS Attribute Screen



- 12 The **Enumerable Attribute Information** screen displays. Select the **802** value from the **Attribute value** drop-down list box.
- Click **OK**.

**Figure 128** 802 Attribute Setting for Tunnel-Medium-Type

Enumerable Attribute Information

Attribute name:  
Tunnel-Medium-Type

Attribute number:  
65

Attribute format:  
Enumerator

Attribute value:  
802 (includes all 802 media plus Ethernet canonical format)

OK Cancel

**13** Return to the **RADIUS Attribute Screen** shown as [Figure 127 on page 207](#).

- Select **Tunnel-Pvt-Group-ID**.
- Click **Add**.

**14** The **Attribute Information** screen displays.

- In the **Enter the attribute value in:** field select **String** and type a number in the range 1 to 4094 or a **Name** for this policy. This **Name** should match a name in the VLAN mapping table on the ZyXEL Device. Wireless stations belonging to the VLAN Group specified in this policy will be given a VLAN **ID** specified in the ZyXEL Device VLAN table.
- Click **OK**.

**Figure 129** VLAN ID Attribute Setting for Tunnel-Pvt-Group-ID

Attribute Information

Attribute name:  
Tunnel-Pvt-Group-ID

Attribute number:  
81

Attribute format:  
OctetString

Enter the attribute value in: ☒ String ☐ Hexadecimal

10

OK Cancel

**15** Return to the **RADIUS Attribute Screen** shown as [Figure 127 on page 207](#).

- Select **Tunnel-Type**.
- Click **Add**.

**16** The **Enumerable Attribute Information** screen displays.

- Select **Virtual LANs (VLAN)** from the attribute value drop-down list box.
- Click **OK**.

**Figure 130** VLAN Attribute Setting for Tunnel-Type

Enumerable Attribute Information

Attribute name:  
Tunnel-Type

Attribute number:  
64

Attribute format:  
Enumerator

Attribute value:  
Virtual LANs (VLAN)

OK Cancel

**17** Return to the **RADIUS Attribute Screen** shown as [Figure 127 on page 207](#).

- Click the **Close** button.
- The completed **Advanced** tab configuration should resemble the following screen.

**Figure 131** Completed Advanced Tab

Allow - VLAN Group 10 Properties

Settings

Policy name:

Specify the condition:  
Windows/Groups in

Add...

If a user matches the condition:  
☒ Grant remote access  
☐ Deny remote access  
 Access will be overridden if the condition is met.

Edit Profile...

Edit Dial-in Profile

Dial-in Constraints | IP | Multilink  
 Authentication | Encryption | Advanced

Specify additional connection attributes to be returned to the Remote Access Server.

Parameters:

| Name                | Vendor          | Value                   |
|---------------------|-----------------|-------------------------|
| Service-Type        | RADIUS Standard | Framed                  |
| Framed-Protocol     | RADIUS Standard | PPP                     |
| Tunnel-Medium-Type  | RADIUS Standard | 802 (includes all 802 m |
| Tunnel-Pvt-Group-ID | RADIUS Standard | 10                      |
| Tunnel-Type         | RADIUS Standard | Virtual LANs (VLAN)     |

Add... Remove Edit...

OK Cancel Apply

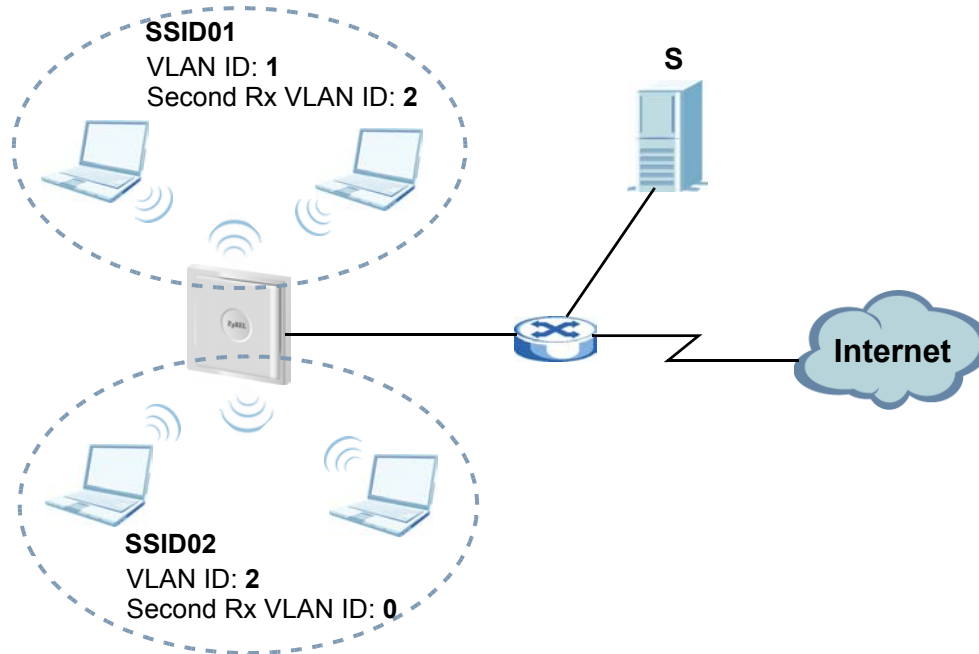


Repeat the Configuring Remote Access Policies procedure for each VLAN Group defined in the Active Directory. Remember to place the most general Remote Access Policies at the bottom of the list and the most specific at the top of the list.

## 16.2.5 Second Rx VLAN ID Example

In this example, the ZyXEL Device is configured to tag packets from **SSID01** with VLAN ID 1 and tag packets from **SSID02** with VLAN ID 2. **VLAN 1** and **VLAN 2** have access to a server, **S**, and the Internet, as shown in the following figure.

**Figure 132** Second Rx VLAN ID Example



Packets sent from the server **S** back to the switch are tagged with a VLAN ID (incoming VLAN ID). These incoming VLAN packets are forwarded to the ZyXEL Device. The ZyXEL Device compares the VLAN ID in the packet header with each SSID's configured VLAN ID and second Rx VLAN ID settings.

In this example, **SSID01**'s second Rx VLAN ID is set to **2**. All incoming packets tagged with VLAN ID **2** are forwarded to **SSID02**, and also to **SSID01**. However, **SSID02** has no second Rx VLAN ID configured, and the ZyXEL Device forwards only packets tagged with VLAN ID **2** to it.

### 16.2.5.1 Second Rx VLAN Setup Example

The following steps show you how to setup a second Rx VLAN ID on the ZyXEL Device.

- 1** Log into the Web Configurator.
- 2** Click **VLAN > Wireless VLAN**.
- 3** If VLAN is not already enabled, click **Enable VIRTUAL LAN** and set up the **Management VLAN ID** (see [Section 16.2.3 on page 199](#)).



If no devices are in the management VLAN, then no one will be able to access the ZyXEL Device and you will have to restore the default configuration file.

- 4 Select the SSID profile you want to configure (**SSID03** in this example), and enter the **VLAN ID** number (between 1 and 4094).
- 5 Enter a **Second Rx VLAN ID**. The following screen shows **SSID03** tagged with a **VLAN ID** of 3 and a **Second Rx VLAN ID** of 4.

Figure 133 Configuring SSID: Second Rx VLAN ID Example

WIRELESS VLAN

RADIUS VLAN

VIRTUAL LAN Setup

☒ Enable VIRTUAL LAN

Wireless VIRTUAL LAN Setup

Management VLAN ID

10

(1 ~ 4094)

VLAN Mapping Table

| Index | Name       | SSID    | VLAN ID       | Second Rx VLAN ID |
|-------|------------|---------|---------------|-------------------|
| 1     | VoIP_SSID  | ZyXEL01 | <div>1</div>  | <div>0</div>      |
| 2     | Guest_SSID | ZyXEL02 | <div>2</div>  | <div>0</div>      |
| 3     | SSID03     | ZyXEL03 | <div>3</div>  | <div>4</div>      |
| 4     | SSID04     | ZyXEL04 | <div>4</div>  | <div>0</div>      |
| 5     | SSID05     | ZyXEL05 | <div>5</div>  | <div>0</div>      |
| 6     | SSID06     | ZyXEL06 | <div></div>   | <div></div>       |
| 7     | SSID07     | ZyXEL07 | <div></div>   | <div></div>       |
| 8     | SSID08     | ZyXEL08 | <div></div>   | <div></div>       |
| 9     | SSID09     | ZyXEL09 | <div></div>   | <div></div>       |
| 10    | SSID10     | ZyXEL10 | <div></div>   | <div></div>       |
| 11    | SSID11     | ZyXEL11 | <div></div>   | <div></div>       |
| 12    | SSID12     | ZyXEL12 | <div></div>   | <div></div>       |
| 13    | SSID13     | ZyXEL13 | <div></div>   | <div></div>       |
| 14    | SSID14     | ZyXEL14 | <div></div>   | <div></div>       |
| 15    | SSID15     | ZyXEL15 | <div>15</div> | <div>0</div>      |
| 16    | SSID16     | ZyXEL16 | <div>16</div> | <div>0</div>      |

Apply

Reset

- 6 Click **Apply** to save these settings. Outgoing packets from clients in **SSID03** are tagged with a **VLAN ID** of 3, and incoming packets with a **VLAN ID** of 3 or 4 are forwarded to **SSID03**.



# Maintenance

This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.

## 17.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your ZyXEL Device.

## 17.2 System Status Screen

Click **MAINTENANCE** to open the **System Status** screen, where you can see information about your ZyXEL Device. Note that the labels in this screen are READ-ONLY and are meant to be used for diagnostic purposes.

**Figure 134** System Status

| Status  | Association List | Channel Usage | F/W Upload | Configuration | Restart |
|---|------------------|---------------|------------|---------------|---------|
| <p>System Name : NWA-Series<br/> ZyNOS Firmware Version : V3.60(AAM.0)b1   02/01/2008</p> <p>IP Address : 192.168.1.2      DHCP : None<br/> IP Subnet Mask : 255.255.255.0</p> <p>Show Statistics</p> |                  |               |            |               |         |

The following table describes the labels in this screen.

**Table 72** System Status

| LABEL                  | DESCRIPTION  |
|------------------------|--|
| System Name            | This is the <b>System Name</b> you can configure in the <b>SYSTEM &gt; General</b> screen. It is for identification purposes |
| ZyNOS Firmware Version | This is the ZyNOS Firmware version and date created. ZyNOS is ZyXEL's proprietary Network Operating System design.           |
| IP Address             | This is the Ethernet port IP address.  |
| IP Subnet Mask         | This is the Ethernet port subnet mask.   |

**Table 72** System Status

| LABEL           | DESCRIPTION  |
|-----------------|--|
| DHCP            | This is the Ethernet port DHCP role - <b>Client</b> or <b>None</b> .   |
| Show Statistics | Click <b>Show Statistics</b> to see router performance statistics such as number of packets sent and number of packets received for each port. |

## 17.2.1 System Statistics

Click **Maintenance > Show Statistics**. Read-only information here includes port status, packet specific statistics and bridge link status. Also provided are "system up time" and "poll interval(s)". The **Poll Interval** field is configurable. The fields in this screen vary according to the current wireless mode.

**Figure 135** System Status: Show Statistics

| Port  | Status    | TxPkts | RxPkts | Collisions | Tx B/s | Rx B/s | Up Time |
|-------|-----------|--------|--------|------------|--------|--------|---------|
| LAN   | 100M/Full | 7147   | 1417   | 0          | 3554   | 937    | 3:26:29 |
| WLAN1 | 54M       | 6817   | 0      | 0          | 0      | 0      | 0:00:45 |
| WLAN2 | 54M       | 6817   | 0      | 0          | 64     | 0      | 0:00:14 |

WLAN1:

| Index | Active | Remote Bridge MAC | Status | TxPkts | RxPkts |
|-------|--------|-------------------|--------|--------|--------|
| 1     | No     | 00:00:00:00:00:00 | Down   | 0      | 0      |
| 2     | No     | 00:00:00:00:00:00 | Down   | 0      | 0      |
| 3     | No     | 00:00:00:00:00:00 | Down   | 0      | 0      |
| 4     | No     | 00:00:00:00:00:00 | Down   | 0      | 0      |
| 5     | No     | 00:00:00:00:00:00 | Down   | 0      | 0      |

WLAN2:

| Index | Active | Remote Bridge MAC | Status | TxPkts | RxPkts |
|-------|--------|-------------------|--------|--------|--------|
| 1     | No     | 00:00:00:00:00:00 | Down   | 0      | 0      |
| 2     | No     | 00:00:00:00:00:00 | Down   | 0      | 0      |
| 3     | No     | 00:00:00:00:00:00 | Down   | 0      | 0      |
| 4     | No     | 00:00:00:00:00:00 | Down   | 0      | 0      |
| 5     | No     | 00:00:00:00:00:00 | Down   | 0      | 0      |

Poll Interval(s) :  sec

The following table describes the labels in this screen.

**Table 73** System Status: Show Statistics

| <b>LABEL</b>      | <b>DESCRIPTION</b>  |
|-------------------|---|
| Port              | This is the Ethernet port ( <b>LAN</b> ) or wireless LAN adaptor ( <b>WLAN1</b> or <b>WLAN2</b> ).  |
| Status            | This shows the port speed and duplex setting if you are using Ethernet encapsulation for the Ethernet port. Ethernet port connections can be in half-duplex or full-duplex mode. Full-duplex refers to a device's ability to send and receive simultaneously, while half-duplex indicates that traffic can flow in only one direction at a time. The Ethernet port must use the same speed or duplex mode setting as the peer Ethernet port in order to connect.<br>This shows the transmission speed only for the wireless adaptors. |
| TxPkts            | This is the number of transmitted packets on this port.   |
| RxPkts            | This is the number of received packets on this port.  |
| Collisions        | This is the number of collisions on this port.  |
| Tx B/s            | This shows the transmission speed in bytes per second on this port.   |
| Rx B/s            | This shows the reception speed in bytes per second on this port.  |
| Up Time           | This is total amount of time the line has been up.  |
| WLAN1             | This section displays only when wireless LAN adaptor WLAN1 is in <b>AP+Bridge</b> or <b>Bridge/Repeater</b> mode.   |
| WLAN2             | This section displays only when wireless LAN adaptor WLAN2 is in <b>AP+Bridge</b> or <b>Bridge/Repeater</b> mode.   |
| Index             | This is the index number of the bridge connection.  |
| Remote Bridge MAC | This is the MAC address of the peer device in bridge mode.  |
| Status            | This shows the current status of the bridge connection, which can be <b>Up</b> or <b>Down</b> .   |
| TxPkts            | This is the number of transmitted packets on the wireless bridge.   |
| RxPkts            | This is the number of received packets on the wireless bridge.  |
| Poll Interval(s)  | Enter the time interval for refreshing statistics.  |
| Set Interval      | Click this button to apply the new poll interval you entered above.   |
| Stop              | Click this button to stop refreshing statistics.  |

## 17.3 Association List

View the wireless stations that are currently associated with the ZyXEL Device in the **Association List** screen.

Click **MAINTENANCE > Association List** to display the screen as shown next.

**Figure 136** Association List

| Status                                 | Association List         | Channel Usage           | F/W Upload      | Configuration | Restart |
|--|--------------------------|-------------------------|-----------------|---------------|---------|
| <b>WLAN1 Stations</b>                  |                          |                         |                 |               |         |
| <b>Index</b>                           | <b>MAC Address</b>       | <b>Association Time</b> | <b>SSID</b>     | <b>Signal</b> |         |
| <b>WDS Link</b>                        |                          |                         |                 |               |         |
| <b>Index</b>                           | <b>Remote Bridge MAC</b> | <b>Link Time</b>        | <b>Security</b> | <b>Signal</b> |         |
| <b>WLAN2 WDS Link</b>                  |                          |                         |                 |               |         |
| <b>Index</b>                           | <b>Remote Bridge MAC</b> | <b>Link Time</b>        | <b>Security</b> | <b>Signal</b> |         |
| <input type="button" value="Refresh"/> |                          |                         |                 |               |         |

The following table describes the labels in this screen.

**Table 74** Association List

| LABEL             | DESCRIPTION   |
|-------------------|---|
| Stations          |   |
| Index             | This is the index number of an associated wireless station.   |
| MAC Address       | This field displays the MAC address of an associated wireless station.  |
| Association Time  | This field displays the time a wireless station first associated with the ZyXEL Device.                           |
| SSID              | This field displays the SSID to which the wireless station is associated.   |
| Signal            | This field displays the RSSI (Received Signal Strength Indicator) of the wireless connection.                     |
| WDS Link          | This section displays only when bridge mode is activated on one of the ZyXEL Device's WLAN adaptors.              |
| Index             | This field displays the index number of a bridge connection on the WDS.   |
| Remote Bridge MAC | This field displays a remote bridge MAC address.  |
| Link Time         | This field displays the WDS link up-time.   |
| Security          | This field displays whether traffic on the WDS is encrypted ( <b>TKIP</b> or <b>AES</b> ) or not ( <b>None</b> ). |
| Refresh           | Click <b>Refresh</b> to reload the screen.  |

## 17.4 Channel Usage

The **Channel Usage** screen shows whether a channel is used by another wireless network or not. If a channel is being used, you should select a channel removed from it by five channels to completely avoid overlap.

Click **MAINTENANCE > Channel Usage** to display the screen shown next.

Wait a moment while the ZyXEL Device compiles the information.

**Figure 137** Channel Usage

| Status             | Association List  | Channel Usage | F/W Upload | Configuration | Restart |
|--------------------|-------------------|---------------|------------|---------------|---------|
|                    |                   |               |            |               |         |
| SSID               | MAC Address       | Channel       | Signal     | Network Mode  |         |
| ZyXEL_1237         | 00:13:49:00:00:01 | 6             | 23 %       | Infra         |         |
| ZyXEL              | 00:13:49:00:00:05 | 6             | 82 %       | Infra         |         |
| Wireless           | 00:A0:C5:00:07:77 | 6             | 42 %       | Infra         |         |
| Wireless           | 00:A0:C5:5C:AF:7A | 11            | 25 %       | Infra         |         |
| A-3214-G3000       | 00:A0:C5:F5:02:06 | 11            | 22 %       | Infra, WEP    |         |
|                    |                   |               |            |               |         |
| <div>Refresh</div> |                   |               |            |               |         |

The following table describes the labels in this screen.

**Table 75** Channel Usage

| LABEL        | DESCRIPTION  |
|--------------|--|
| SSID         | This is the Service Set IDentification name of the AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network. For our purposes, we define an Infrastructure network as a wireless network that uses an AP and an Ad-Hoc network (also known as Independent Basic Service Set (IBSS)) as one that doesn't. See the chapter on wireless configuration for more information on basic service sets (BSS) and extended service sets (ESS). |
| MAC Address  | This field displays the MAC address of the AP in an Infrastructure wireless network. It is randomly generated (so ignore it) in an Ad-Hoc wireless network.  |
| Channel      | This is the index number of the channel currently used by the associated AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network.   |
| Signal       | This field displays the strength of the AP's signal. If you must choose a channel that's currently in use, choose one with low signal strength for minimum interference.   |
| Network Mode | "Network mode" in this screen refers to your wireless LAN infrastructure (refer to the Wireless LAN chapter) and security setup.   |
| Refresh      | Click <b>Refresh</b> to reload the screen.   |

## 17.5 F/W Upload Screen

Find firmware at [www.zyxel.com](http://www.zyxel.com) in a file that (usually) uses the system model name with a "\*.bin" extension, for example "NWA-Series.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See the Firmware and Configuration File Maintenance chapter for upgrading firmware using FTP/TFTP commands.

Click **MAINTENANCE > F/W Upload**. Follow the instructions in this screen to upload firmware to your ZyXEL Device.

**Figure 138** Firmware Upload

The following table describes the labels in this screen.

**Table 76** Firmware Upload

| LABEL     | DESCRIPTION  |
|-----------|--|
| File Path | Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.   |
| Browse... | Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them. |
| Upload    | Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.  |



**Do not turn off the ZyXEL Device while firmware upload is in progress!**

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the ZyXEL Device again.

**Figure 139** Firmware Upload In Process

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 140** Network Temporarily Disconnected

After two minutes, log in again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

**Figure 141** Firmware Upload Error

## 17.6 Configuration Screen

See [Chapter 23 on page 243](#) for information on how to transfer configuration files using FTP/TFTP commands.

Click **MAINTENANCE > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

**Figure 142** Configuration

The screenshot shows a web interface with a top navigation bar containing tabs: Status, Association List, Channel Usage, F/W Upload, Configuration (selected), and Restart. The main content area has three sections:

- Backup Configuration:** A heading followed by the instruction "Click Backup to save the current configuration of your system to your computer." and a "Backup" button.
- Restore Configuration:** A heading followed by the instruction "To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload." Below this is a "File Path:" label, an empty text input field, a "Browse..." button, and an "Upload" button.
- Back to Factory Defaults:** A heading followed by the instruction "Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the" and a bulleted list:
  - Password will be 1234
  - This device can be reached by IP address 192.168.1.2
 Below the list is a "Reset" button.

### 17.6.1 Backup Configuration

Backup configuration allows you to back up (save) the ZyXEL Device's current configuration to a file on your computer. Once your ZyXEL Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the ZyXEL Device's current configuration to your computer.

### 17.6.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your ZyXEL Device.

**Table 77** Restore Configuration

| LABEL     | DESCRIPTION   |
|-----------|---|
| File Path | Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.  |
| Browse... | Click <b>Browse...</b> to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them. |
| Upload    | Click <b>Upload</b> to begin the upload process.  |



**Do not turn off the ZyXEL Device while configuration file upload is in progress.**

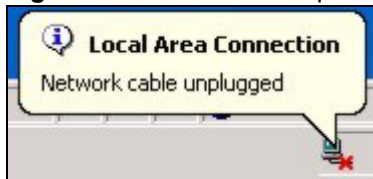
After you see a “restore configuration successful” screen, you must then wait one minute before logging into the ZyXEL Device again.

**Figure 143** Configuration Upload Successful



The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

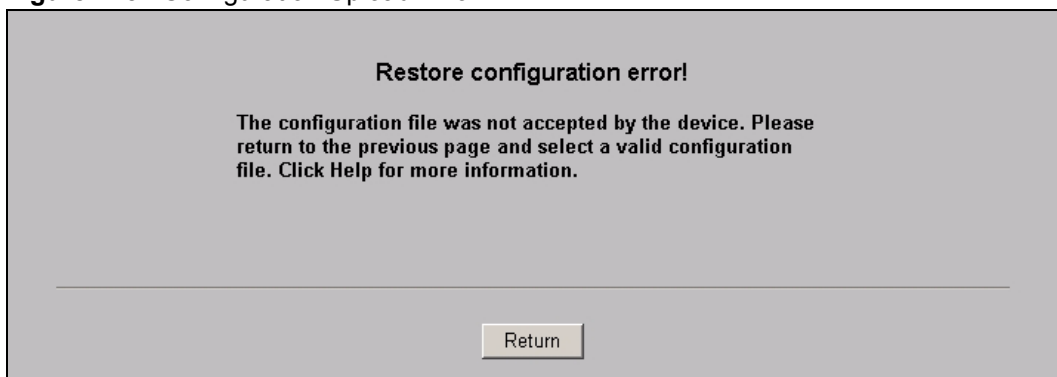
**Figure 144** Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default ZyXEL Device IP address (192.168.1.2). See your Quick Start Guide for details on how to set up your computer’s IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

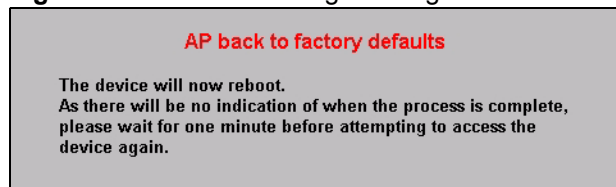
**Figure 145** Configuration Upload Error



### 17.6.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the ZyXEL Device to its factory defaults as shown on the screen. The following warning screen will appear.

**Figure 146** Reset Warning Message



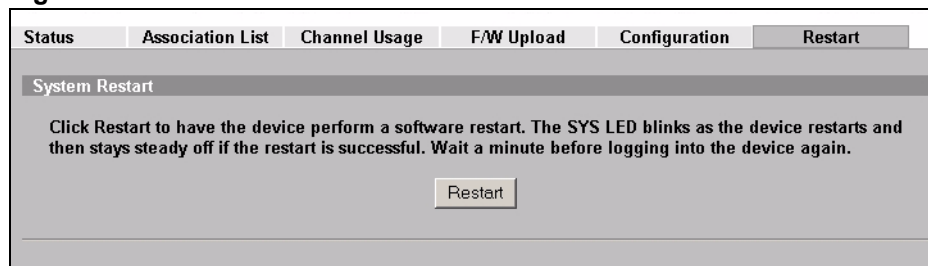
You can also press the **RESET** button to reset your ZyXEL Device to its factory default settings. Refer to [Section 2.2 on page 42](#) for more information.

## 17.7 Restart Screen

System restart allows you to reboot the ZyXEL Device without turning the power off.

Click **MAINTENANCE > Restart**. Click **Restart** to have the ZyXEL Device reboot. This does not affect the ZyXEL Device's configuration.

**Figure 147** Restart Screen



---

# **PART III**

## **SMT,**

# **Troubleshooting and Specifications**

---

Introducing the SMT (225)

General Setup (231)

LAN Setup (233)

System Password (235)

System Password (235)

System Information and Diagnosis (237)

Firmware and Configuration File Maintenance (243)

System Maintenance and Information (249)

Troubleshooting (257)

Product Specifications (261)



# Introducing the SMT

This chapter describes how to access the SMT and provides an overview of its menus.

## 18.1 Introduction to the SMT

The ZyXEL Device's SMT (System Management Terminal) is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection. This chapter shows you how to access the SMT (System Management Terminal) menus, how to navigate the SMT and how to configure SMT menus.

## 18.2 Accessing the SMT via the Console Port

Use the console port to configure the ZyXEL Device via SMT menus. Connect the PS/2 connector of the console cable to the console port of the ZyXEL Device and the other end to a serial port (COM1, COM2 or other COM port) on your computer.

When configuring using the console port, you need a computer equipped with communications software configured to the following parameters:

- VT100 terminal emulation.
- 9600 Baud.
- No parity, 8 data bits, 1 stop bit, flow control set to none.

### 18.2.1 Initial Screen

When you turn on your ZyXEL Device, it performs several internal tests.

After the tests, the ZyXEL Device asks you to press [ENTER] to continue, as shown next.

**Figure 148** Initial Screen

```

Bootbase Version: V1.05 | 03/23/2007 11:39:53
RAM:Size = 32 Mbytes
DRAM POST: Testing: 32608K OK
DRAM Test SUCCESS !
FLASH: AMD 32M

ZyNOS Version: V3.60(AAM.0)b1 | 02/01/2008 19:40:56

Press any key to enter debug mode within 3 seconds.
.....
..

Copyright (c) 1994 - 2007 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:13:49:DF:42:A8
initialize ch =1, ethernet address: 00:13:49:DF:42:A8
initialize ch =2, ethernet address: 00:13:49:DF:42:A9
initialize ch =3, ethernet address: 06:13:49:DF:42:A8
initialize ch =4, ethernet address: 0A:13:49:DF:42:A8
initialize ch =5, ethernet address: 0E:13:49:DF:42:A8
initialize ch =6, ethernet address: 12:13:49:DF:42:A8
initialize ch =7, ethernet address: 16:13:49:DF:42:A8
initialize ch =8, ethernet address: 1A:13:49:DF:42:A8
initialize ch =9, ethernet address: 1E:13:49:DF:42:A8
initialize ch =10, ethernet address: 06:13:49:DF:42:A9
initialize ch =11, ethernet address: 0A:13:49:DF:42:A9
initialize ch =12, ethernet address: 0E:13:49:DF:42:A9
initialize ch =13, ethernet address: 12:13:49:DF:42:A9
initialize ch =14, ethernet address: 16:13:49:DF:42:A9
initialize ch =15, ethernet address: 1A:13:49:DF:42:A9
initialize ch =16, ethernet address: 1E:13:49:DF:42:A9
initialize ch =17, ethernet address: 00:13:49:DF:42:A8
initialize ch =18, ethernet address: 00:13:49:DF:42:A8
initialize ch =19, ethernet address: 00:13:49:DF:42:A8
initialize ch =20, ethernet address: 00:13:49:DF:42:A8
initialize ch =21, ethernet address: 00:13:49:DF:42:A8
initialize ch =22, ethernet address: 00:13:49:DF:42:A9
initialize ch =23, ethernet address: 00:13:49:DF:42:A9
initialize ch =24, ethernet address: 00:13:49:DF:42:A9
initialize ch =25, ethernet address: 00:13:49:DF:42:A9
initialize ch =26, ethernet address: 00:13:49:DF:42:A9
Press ENTER to continue...

```

## 18.2.2 Entering the Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown below.

For your first login, enter the default password “1234”. As you type the password, the screen displays an “X” for each character you type.



Whether or not you use administrator authentication on RADIUS, you still use the local system password to log in via the console port.

Please note that if there is no activity for longer than five minutes after you log in, your ZyXEL Device will automatically log you out and display a blank screen. If you see a blank screen, press [ENTER] to bring up the login screen again.

**Figure 149** Password Screen

Enter Password : XXXX

## 18.3 Connect to your ZyXEL Device Using Telnet

The following procedure details how to telnet into your ZyXEL Device.

- 1 In Windows, click **Start** (usually in the bottom left corner), **Run** and then type “telnet 192.168.1.2” (the default IP address) and click **OK**.
- 2 For your first login, enter the default password “1234”. As you type the password, the screen displays an asterisk “\*” for each character you type.

**Figure 150** Login Screen

Password : xxxx

- 3 After entering the password you will see the main menu.

Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your ZyXEL Device will automatically log you out. You will then have to telnet into the ZyXEL Device again. You can use the web configurator or the CLI commands to change the inactivity time out period.

## 18.4 Changing the System Password

Change the ZyXEL Device’s default password by following the steps shown next.

- 1 From the main menu, enter “23” to display **Menu 23 – System Password**.
- 2 Type your existing system password in the **Old Password** field, and press [ENTER].

Figure 151 Menu 23 System Password

Menu 23 - System Password

Old Password= \*\*\*\*

New Password= ?

Retype to confirm= ?

Enter here to CONFIRM or ESC to CANCEL:

- 3 Type your new system password in the **New Password** field (up to 30 characters), and press [ENTER].
- 4 Re-type your new system password in the **Retype to confirm** field for confirmation and press [ENTER].

Note that as you type a password, the screen displays an asterisk “\*” for each character you type.

## 18.5 SMT Menu Overview Example

The following table gives you an overview of your ZyXEL Device’s various SMT menus.

Table 78 SMT Menus Overview

| MENUS                 | SUB MENUS                                      |                           |
|-----------------------|--|---------------------------|
| 1 General Setup       |  |                           |
| 3 LAN Setup           | 3.2 TCP/IP Setup                               |                           |
| 23 System Password    |  |                           |
| 24 System Maintenance | 24.1 System Status                             |                           |
|                       | 24.2 System Information and Console Port Speed | 24.2.1 System Information |
|                       |  | 24.2.2 Console Port Speed |
|                       | 24.3 Log and Trace                             |                           |
|                       | 24.4 Diagnostic                                |                           |
|                       | 24.8 Command Interpreter Mode                  |                           |
|                       | 24.10 Time and Date Setting                    |                           |
|                       | 24.11 Remote Management Setup                  |                           |

## 18.6 Navigating the SMT Interface

The SMT (System Management Terminal) is the interface that you use to configure your ZyXEL Device.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

**Table 79** Main Menu Commands

| OPERATION                  | KEYSTROKE   | DESCRIPTION   |
|----------------------------|---|---|
| Move down to another menu  | [ENTER]   | To move forward to a submenu, type in the number of the desired submenu and press [ENTER].  |
| Move up to a previous menu | [ESC]   | Press [ESC] to move back to the previous menu.  |
| Move to a "hidden" menu    | Press [SPACE BAR] to change <b>No</b> to <b>Yes</b> then press [ENTER]. | Fields beginning with "Edit" lead to hidden menus and have a default setting of <b>No</b> . Press [SPACE BAR] once to change <b>No</b> to <b>Yes</b> , then press [ENTER] to go to the "hidden" menu.         |
| Move the cursor            | [ENTER] or [UP]/[DOWN] arrow keys.                                      | Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.   |
| Entering information       | Type in or press [SPACE BAR], then press [ENTER].                       | You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].                 |
| Required fields            | <?> or <b>ChangeMe</b>  | All fields with the symbol <?> must be filled in order to be able to save the new configuration.<br>All fields with <b>ChangeMe</b> must not be left blank in order to be able to save the new configuration. |
| N/A fields                 | <N/A>   | Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.  |
| Save your configuration    | [ENTER]   | Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu.                        |
| Exit the SMT               | Type "99", then press [ENTER].  | Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.  |

After you enter the password, the SMT displays the main menu, as shown next.

**Figure 152** SMT Main Menu

|  |                        |
|--|------------------------|
| Copyright (c) 1994 - 2007 ZyXEL Communications Corp. |                        |
| NWA3550 Main Menu                                    |                        |
| Getting Started                                      | Advanced Management    |
| 1. General Setup                                     | 23. System Security    |
| 3. LAN Setup   | 24. System Maintenance |
|  | 99. Exit               |
| Enter Menu Selection Number:                         |                        |

## 18.6.1 System Management Terminal Interface Summary

**Table 80** Main Menu Summary

| #  | MENU TITLE         | DESCRIPTION  |
|----|--------------------|--|
| 1  | General Setup      | Use this menu to set up your general information.                    |
| 3  | LAN Setup          | Use this menu to set up your LAN and WLAN connection.                |
| 23 | System Password    | Use this menu to change your password.                               |
| 24 | System Maintenance | This menu provides system status, diagnostics, software upload, etc. |
| 99 | Exit               | Use this to exit the SMT.  |

# General Setup

The chapter shows you the information on general setup.

## 19.1 General Setup

**Menu 1 – General Setup** contains administrative and system-related information (shown next). The **System Name** field is for identification purposes.

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the ZyXEL Device via DHCP.

### 19.1.1 Procedure To Configure Menu 1

Enter “1” in the Main Menu to open **Menu 1 – General Setup** as shown next.

**Figure 153** Menu 1 General Setup

|   |
|---|
| <p style="text-align: center;">Menu 1 - General Setup</p> <p>System Name= NWA-Series</p> <p>Domain Name=</p> <p>First System DNS Server= None</p> <p>IP Address= N/A</p> <p>Second System DNS Server= None</p> <p>IP Address= N/A</p> <p>Third System DNS Server= None</p> <p>IP Address= N/A</p> |
|---|

Fill in the required fields. Refer to the following table for more information about these fields.

**Table 81** Menu 1 General Setup

| FIELD       | DESCRIPTION   |
|-------------|---|
| System Name | Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes “-” and underscores “_” are accepted. |
| Domain Name | This is not a required field. Leave this field blank or enter the domain name here if you know it.  |

**Table 81** Menu 1 General Setup

| FIELD  | DESCRIPTION   |
|--|---|
| First/Second/Third System DNS Server   | Press [SPACE BAR] to select <b>From DHCP</b> , <b>User Defined</b> or <b>None</b> and press [ENTER].<br>These fields are not available on all models. |
| IP Address   | Enter the IP addresses of the DNS servers. This field is available when you select <b>User-Defined</b> in the field above.                            |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel. |   |

## LAN Setup

This chapter shows you how to configure the LAN on your ZyXEL Device.

### 20.1 LAN Setup

This section describes how to configure the Ethernet using **Menu 3 – LAN Setup**. From the main menu, enter “3” to display menu 3.

**Figure 154 Menu 3 LAN Setup**

```
Menu 3 - LAN Setup

2. TCP/IP Setup

Enter Menu Selection Number:
```

Detailed explanation about the LAN Setup menu is given in the next chapter.

### 20.2 TCP/IP Ethernet Setup

Use menu 3.2 to configure your ZyXEL Device for TCP/IP.

To edit menu 3.2, enter “3” from the main menu to display **Menu 3-LAN Setup**. When menu 3 appears, type “2” and press [ENTER] to display **Menu 3.2-TCP/IP Setup**, as shown next:

**Figure 155 Menu 3.2 TCP/IP Setup**

```
Menu 3.2 - TCP/IP Setup

IP Address Assignment= Static
IP Address= 192.168.1.2
IP Subnet Mask= 255.255.255.0
Gateway IP Address= 0.0.0.0
```

Follow the instructions in the following table on how to configure the fields in this menu.

**Table 82** Menu 3.2 TCP/IP Setup

| FIELD  | DESCRIPTION   |
|--|---|
| IP Address Assignment  | Press [SPACE BAR] and then [ENTER] to select <b>Dynamic</b> to have the ZyXEL Device obtain an IP address from a DHCP server. You must know the IP address assigned to the ZyXEL Device (by the DHCP server) to access the ZyXEL Device again.<br>Select <b>Static</b> to give the ZyXEL Device a fixed, unique IP address. Enter a subnet mask appropriate to your network and the gateway IP address if applicable. |
| IP Address   | Enter the (LAN) IP address of your ZyXEL Device in dotted decimal notation  |
| IP Subnet Mask   | Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.   |
| Gateway IP Address   | Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyXEL Device that will forward the packet to the destination. On the LAN, the gateway must be a router on the same network segment as your ZyXEL Device.   |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel. |   |

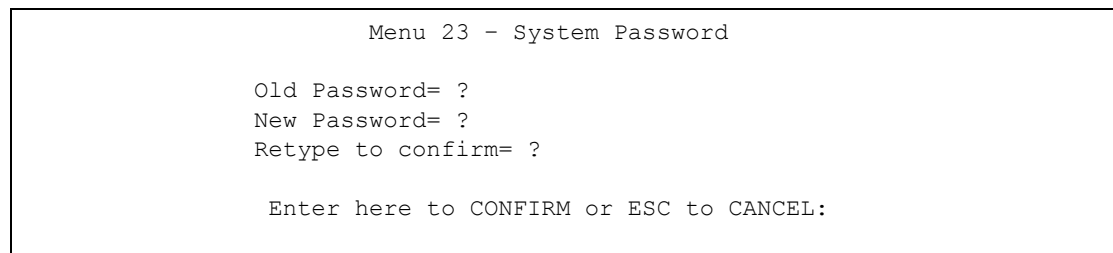
# System Password

This chapter describes how to configure the ZyXEL Device's system password.

## 21.1 System Password

You can configure the system password in this menu. Refer to [Section 18.4 on page 227](#).

**Figure 156** Menu 23 System Password



The screenshot shows a text-based menu titled "Menu 23 - System Password". Below the title, there are three lines of text: "Old Password= ?", "New Password= ?", and "Retype to confirm= ?". At the bottom of the menu, there is a line of text: "Enter here to CONFIRM or ESC to CANCEL:". The entire menu is enclosed in a rectangular border.

```
Menu 23 - System Password

Old Password= ?
New Password= ?
Retype to confirm= ?

Enter here to CONFIRM or ESC to CANCEL:
```

You should change the default password. If you forget your password you have to restore the default configuration file. Refer to [Section 2.2 on page 42](#).



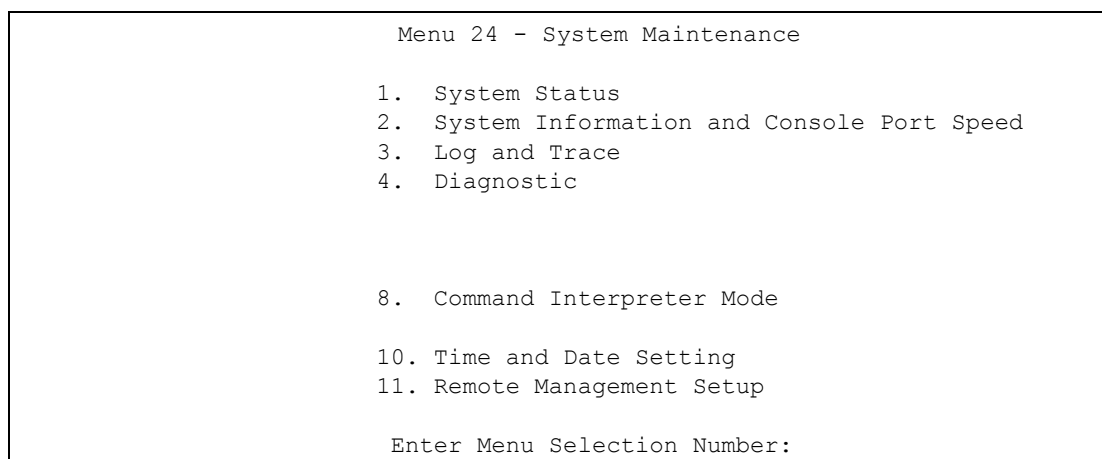
# System Information and Diagnosis

This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.4.

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type “24” in the main menu and press [ENTER] to open **Menu 24 – System Maintenance**, as shown in the following figure.

**Figure 157** Menu 24 System Maintenance



## 22.1 System Status

The first selection, **System Status** gives you information on the status and statistics of the ports, as shown next. **System Status** is a tool that can be used to monitor your ZyXEL Device. Specifically, it gives you information on your Ethernet and Wireless LAN status, and the number of packets sent and received.

To get to **System Status**, type “24” to go to **Menu 24 – System Maintenance**. From this menu, type “1”. There are two commands in **Menu 24.1 – System Maintenance – Status**. Entering 9 resets the counters; pressing [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 – System Maintenance – Status** which are read-only and meant for diagnostic purposes.

**Figure 158 Menu 24.1 System Maintenance: Status**

|  |                   |        |             |      |               |        |                    |
|--|-------------------|--------|-------------|------|---------------|--------|--------------------|
| Menu 24.1 - System Maintenance - Status        |                   |        |             |      |               |        | 00:15:06           |
|  |                   |        |             |      |               |        | Sat. Jan. 01, 2000 |
| Port   | Status            | TxPkts | RxPkts      | Cols | Tx B/s        | Rx B/s | Up Time            |
| Ethernet                                       | 100M/Full         | 761    | 366         | 0    | 305           | 192    | 0:15:01            |
| WLAN1  | 54M               | 515    | 0           | 0    | 64            | 0      | 0:15:04            |
| WLAN2  | Down              | 0      | 0           | 0    | 0             | 0      | 0:00:00            |
| Port   | Ethernet Address  |        | IP Address  |      | IP Mask       |        | DHCP               |
| Ethernet                                       | 00:13:49:00:00:01 |        | 192.168.1.2 |      | 255.255.255.0 |        | None               |
| WLAN1  | 00:13:49:00:00:01 |        |             |      |               |        |                    |
| WLAN2  | 00:13:49:00:00:02 |        |             |      |               |        |                    |
| System up Time: 0:15:09                        |                   |        |             |      |               |        |                    |
| ZyNOS F/W Version: V3.60(AAM.0)b1   02/01/2008 |                   |        |             |      |               |        |                    |
| Name: NWA-Series                               |                   |        |             |      |               |        |                    |
| Press Command:                                 |                   |        |             |      |               |        |                    |
| COMMANDS: 9-Reset Counters ESC-Exit            |                   |        |             |      |               |        |                    |

The following table describes the fields present in this menu.

**Table 83 Menu 24.1 System Maintenance: Status**

| FIELD             | DESCRIPTION  |
|-------------------|--|
| Port              | This is the port type. Port types are: Ethernet, WLAN1 and WLAN2.  |
| Status            | This shows the status of the remote node.  |
| TxPkts            | This is the number of transmitted packets to this remote node.   |
| RxPkts            | This is the number of received packets from this remote node.  |
| Cols              | This is the number of collisions on this connection.   |
| Tx B/s            | This shows the transmission rate in bytes per second.  |
| Rx B/s            | This shows the receiving rate in bytes per second.   |
| Up Time           | This is the time this channel has been connected to the current remote node.   |
| Ethernet Address  | This shows the MAC address of the port.  |
| IP Address        | This shows the IP address of the network device connected to the port.   |
| IP Mask           | This shows the subnet mask of the network device connected to the port.  |
| DHCP              | This shows the DHCP setting (None or Client) for the port.   |
| System Up Time    | This is the time the ZyXEL Device is up and running from the last reboot.  |
| ZyNOS F/W Version | Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation. |
| Name              | This displays the device name.   |

## 22.2 System Information

To get to the System Information:

- 1 Enter “24” to display **Menu 24 – System Maintenance**.
- 2 Enter “2” to display **Menu 24.2 – System Information and Console Port Speed**.
- 3 From this menu you have two choices as shown in the next figure:

**Figure 159** Menu 24.2 System Information and Console Port Speed

```

Menu 24.2 - System Information and Console Port Speed
  1. System Information
  2. Console Port Speed

Please enter selection:

```



The ZyXEL Device also has an internal console port for support personnel only. Do not open the ZyXEL Device as it will void your warranty.

## 22.2.1 System Information

Enter “1” in menu 24.2 to display the screen shown next.

**Figure 160** Menu 24.2.1 System Information: Information

```

Menu 24.2.1 - System Maintenance - Information

Name: NWA-Series
Routing: BRIDGE
ZyNOS F/W Version: V3.60 (AAM.0)b1 | 02/01/2008
Country Code:

LAN
Ethernet Address: 00:13:49:00:00:01
IP Address: 192.168.1.2
IP Mask: 255.255.255.0
DHCP: None

Press ESC or RETURN to Exit:

```

The following table describes the fields in this menu.

**Table 84** Menu 24.2.1 System Maintenance: Information

| FIELD             | DESCRIPTION  |
|-------------------|--|
| Name              | Displays the system name of your ZyXEL Device. This information can be changed in <b>Menu 1 – General Setup</b> .                                  |
| Routing           | Refers to the routing protocol used.   |
| ZyNOS F/W Version | Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation. |

**Table 84** Menu 24.2.1 System Maintenance: Information

| FIELD  | DESCRIPTION   |
|--|---|
| Country Code   | Refers to the country code of the firmware.                             |
| LAN  |   |
| Ethernet Address   | Refers to the Ethernet MAC (Media Access Control) of your ZyXEL Device. |
| IP Address   | This is the IP address of the ZyXEL Device in dotted decimal notation.  |
| IP Mask  | This shows the subnet mask of the ZyXEL Device.                         |
| DHCP   | This field shows the DHCP setting of the ZyXEL Device.                  |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen. |   |

## 22.2.2 Console Port Speed

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your ZyXEL Device supports 9600 (default), 19200, 38400, 57600 and 115200 bps console port speeds. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

**Figure 161** Menu 24.2.2 System Maintenance: Change Console Port Speed

```

Menu 24.2.2 - System Maintenance - Change Console Port Speed

      Console Port Speed: 9600

      Press ENTER to Confirm or ESC to Cancel:

```

After you changed your ZyXEL Device's console port speed, you must also make the same change to the console port speed parameter of your communication software.

## 22.3 Log and Trace

Your ZyXEL Device provides error logs and trace records that are stored locally.

### 22.3.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error log. Follow the procedures to view the local error/trace log:

- 1 Type "24" in the main menu to display **Menu 24 – System Maintenance**.
- 2 From menu 24, type "3" to display **Menu 24.3 – System Maintenance – Log and Trace**.

**Figure 162** Menu 24.3 System Maintenance: Log and Trace

```

Menu 24.3 - System Maintenance - Log and Trace
      1. View Error Log
      Please enter selection:

```

- 3 Enter 1 from **Menu 24.3 – System Maintenance – Log and Trace** and press [ENTER] twice to display the error log in the system.

After the ZyXEL Device finishes displaying the error log, you will have the option to clear it. Samples of typical error and information messages are presented in the next figure.

**Figure 163** Sample Error and Information Messages

```

55 Sat Jan 1 00:00:00 2000 PP05 ERROR Wireless LAN init fail, code=-1
56 Sat Jan 1 00:00:01 2000 PP07 INFO LAN promiscuous mode <1>
57 Sat Jan 1 00:00:01 2000 PINI INFO Last errorlog repeat 1 Times
58 Sat Jan 1 00:00:01 2000 PINI INFO main: init completed
59 Sat Jan 1 00:00:02 2000 PP05 -WARN SNMP TRAP 3: link up
60 Sat Jan 1 00:00:30 2000 PSSV -WARN SNMP TRAP 0: cold start
61 Sat Jan 1 00:01:38 2000 PINI INFO SMT Session Begin
62 Sat Jan 1 00:06:44 2000 PINI INFO SMT Session End
63 Sat Jan 1 00:11:13 2000 PINI INFO SMT Session Begin
Clear Error Log (y/n):

```

## 22.4 Diagnostic

The diagnostic facility allows you to test the different aspects of your ZyXEL Device to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in the following figure.

**Figure 164** Menu 24.4 System Maintenance: Diagnostic

```

Menu 24.4 - System Maintenance - Diagnostic

TCP/IP
  1. Ping Host
  2. DHCP Release
  3. DHCP Renewal

System
  11. Reboot System

Enter Menu Selection Number:
Host IP Address= N/A

```

Follow the procedure next to display this menu:

- 1 From the main menu, type “24” to open **Menu 24 – System Maintenance**.
- 2 From this menu, type “4” to open **Menu 24.4 – System Maintenance – Diagnostic**.

The following table describes the diagnostic tests available in menu 24.4 for your ZyXEL Device and the connections.

**Table 85** Menu 24.4 System Maintenance Menu: Diagnostic

| FIELD           | DESCRIPTION   |
|-----------------|---|
| Ping Host       | Ping the host to see if the links and TCP/IP protocol on both systems are working.    |
| DHCP Release    | Release the IP address assigned by the DHCP server.                                   |
| DHCP Renewal    | Get a new IP address from the DHCP server.  |
| Reboot System   | Reboot the ZyXEL Device.  |
| Host IP Address | If you typed "1" to Ping Host, now type the address of the computer you want to ping. |

# Firmware and Configuration File Maintenance

This chapter tells you how to backup and restore your configuration file as well as upload new firmware and configuration files using the SMT screens.

## 23.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password and TCP/IP Setup, etc. It arrives from ZyXEL with a rom filename extension. Once you have customized the ZyXEL Device's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the ZyXEL Device.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file config.cfg.

If your [T]FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyXEL Device only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyXEL Device and the external filename refers to the filename not on the ZyXEL Device, that is, on your computer, local network or FTP site and so the name (but not the extension) will vary. After uploading new firmware see the **ZyNOS F/W Version** field in **Menu 24.2.1 – System Maintenance – Information** to confirm that you have uploaded the correct firmware version.

**Table 86** Filename Conventions

| FILE TYPE          | INTERNAL NAME | EXTERNAL NAME | DESCRIPTION  |
|--------------------|---------------|---------------|--|
| Configuration File | Rom-0         | *.rom         | This is the configuration filename on the ZyXEL Device. Uploading the rom-0 file replaces the entire ROM file system, including your ZyXEL Device configurations, system-related data (including the default password), the error log and the trace log. |
| Firmware           | Ras           | *.bin         | This is the generic name for the ZyNOS firmware on the ZyXEL Device.   |

## 23.2 Backup Configuration

Backup is highly recommended once your ZyXEL Device is functioning properly. FTP is the preferred method, although TFTP can also be used.

Please note that the terms “download” and “upload” are relative to the computer. Download means to transfer from the ZyXEL Device to the computer, while upload means from your computer to the ZyXEL Device.

### 23.2.1 Using the FTP command from the DOS Prompt

- 1 Launch the FTP client on your computer.
- 2 Enter “open” and the IP address of your ZyXEL Device.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter “root” and your SMT password as requested. The default is 1234.
- 5 Enter “bin” to set transfer mode to binary.
- 6 Use “get” to transfer files from the ZyXEL Device to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the ZyXEL Device to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.
- 7 Enter “quit” to exit the FTP prompt.

**Figure 165** FTP Session Example

```

331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 327680 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit

```

The following table describes some of the commands that you may see in third party FTP clients.

**Table 87** General Commands for Third Party FTP Clients

| COMMAND                  | DESCRIPTION   |
|--------------------------|---|
| Host Address             | Enter the address of the host server.   |
| Login Type               | Anonymous.<br>This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option.<br>Normal.<br>The server requires a unique User ID and Password to login. |
| Transfer Type            | Transfer files in either ASCII (plain text format) or in binary mode.   |
| Initial Remote Directory | Specify the default remote directory (path).  |
| Initial Local Directory  | Specify the default local directory (path).   |

### 23.2.2 Backup Configuration Using TFTP

The ZyXEL Device supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next:

- 1 Use telnet from your computer to connect to the ZyXEL Device and log in. Because TFTP does not have any security checks, the ZyXEL Device records the IP address of the telnet client and accepts TFTP requests only from this address.
- 2 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- 3 Enter command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.
- 4 Launch the TFTP client on your computer and connect to the ZyXEL Device. Set the transfer mode to binary before starting data transfer.

- 5 Use the TFTP client (see the example below) to transfer files between the ZyXEL Device and the computer. The file name for the configuration file is `rom-0` (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyXEL Device to the computer and “binary” to set binary transfer mode.

### 23.2.3 Example: TFTP Command

The following is an example TFTP command:

```
TFTP [-i] host get rom-0 config.rom
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyXEL Device IP address, “get” transfers the file source on the ZyXEL Device (rom-0 name of the configuration file on the ZyXEL Device) to the file destination on the computer and renames it config.rom.

The following table describes some of the fields that you may see in third party TFTP clients.

**Table 88** General Commands for Third Party TFTP Clients

| COMMAND     | DESCRIPTION  |
|-------------|--|
| Host        | Enter the IP address of the ZyXEL Device. 192.168.1.2 is the ZyXEL Device's default IP address when shipped.                 |
| Send/Fetch  | Use “Send” to upload the file to the ZyXEL Device and “Fetch” to back up the file on your computer.                          |
| Local File  | Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.     |
| Remote File | This is the filename on the ZyXEL Device. The filename for the firmware is “ras” and for the configuration file, is “rom-0”. |
| Binary      | Transfer the file in binary mode.  |
| Abort       | Stop transfer of the file.   |

## 23.3 Restore Configuration

You can restore the configuration via FTP or TFTP to your ZyXEL Device. The preferred method is FTP. Note that this function erases the current configuration before restoring the previous backup configuration; please do not attempt to restore unless you have a backup configuration stored on disk. To restore configuration using FTP or TFTP is the same as uploading the configuration file, please refer to the following sections on FTP and TFTP file transfer for more details. The ZyXEL Device restarts automatically after the file transfer is complete.

### 23.3.1 Using the FTP command from the DOS Prompt Example

- 1 Launch the FTP client on your computer.
- 2 Enter “open” and the IP address of your ZyXEL Device.
- 3 Press [ENTER] when prompted for a username.

- 4 Enter “root” and your SMT password as requested. The default is 1234.
- 5 Enter “bin” to set transfer mode to binary.
- 6 Use “put” to transfer files from the computer to the ZyXEL Device for example “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the ZyXEL Device and renames it “ras”. Similarly “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the ZyXEL Device and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the ZyXEL Device to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
- 7 Enter “quit” to exit the FTP prompt.

**Figure 166** FTP Session Example

```

331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 327680 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit

```

More commands that you may find in third party FTP clients are listed earlier in this chapter.

### 23.3.2 TFTP File Upload

The ZyXEL Device also supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next:

- 1 Use telnet from your computer to connect to the ZyXEL Device and log in. Because TFTP does not have any security checks, the ZyXEL Device records the IP address of the telnet client and accepts TFTP requests only from this address.
- 2 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- 3 Enter the command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.
- 4 Launch the TFTP client on your computer and connect to the ZyXEL Device. Set the transfer mode to binary before starting data transfer.
- 5 Use the TFTP client (see the example below) to transfer files between the ZyXEL Device and the computer. The file name for the firmware is “ras” and the configuration file is “rom-0” (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyXEL Device to the computer, “put” the other way around, and “binary” to set binary transfer mode.

### 23.3.3 Example: TFTP Command

The following is an example TFTP command:

```
TFTP [-i] host put firmware.bin ras
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyXEL Device’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the ZyXEL Device).

Commands that you may see in third party TFTP clients are listed earlier in this chapter.

# System Maintenance and Information

This chapter leads you through SMT menus 24.8 and 24.10.

## 24.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the [zyxel.com](http://zyxel.com) web site for more detailed information on CI commands. Enter 8 from **Menu 24 – System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type “exit” to return to the SMT main menu when finished.



Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

**Figure 167** Menu 24 System Maintenance

```
Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic

8. Command Interpreter Mode

10. Time and Date Setting
11. Remote Management Setup

Enter Menu Selection Number:
```



Not all commands are available in all models.

**Figure 168** Valid CI Commands

```
Copyright (c) 1994 - 2007 ZyXEL Communications Corp.
NWA-Serie> help or ?
Valid commands are:
sys          exit          device        ether
config       wlan          ip            ppp
bridge       hdap          bm            certificates
netsnmp     radius        8021x        radserv
wcfg         rogueAP
NWA-Serie>
```

## 24.1.1 Command Syntax

- The command keywords are in `courier new` font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets `<>`.
- The optional fields in a command are enclosed in square brackets `[ ]`.
- The `|` symbol means or.

For example,

`sys filter netbios config <type> <on|off>`

means that you must specify the type of netbios filter and whether to turn it on or off.

## 24.1.2 Command Usage

A list of valid commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

## 24.1.3 Brute-Force Password Guessing Protection

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password.

**Table 89** Brute-Force Password Guessing Protection Commands

| COMMAND                      | DESCRIPTION   |
|------------------------------|---|
| <code>sys pwdertrtm</code>   | This command displays the brute-force guessing password protection settings.  |
| <code>sys pwdertrtm 0</code> | This command turns off the password's protection from brute-force guessing. The brute-force password guessing protection is turned off by default.                  |
| <code>sys pwdertrtm N</code> | This command sets the password protection to block all access attempts for N (a number from 1 to 60) minutes after the third time an incorrect password is entered. |

### 24.1.3.1 Configuring Brute-Force Password Guessing Protection: Example

```
sys pwdertrtm 5
```

This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.

## 24.2 Time and Date Setting

The ZyXEL Device keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyXEL Device. Menu 24.10 allows you to update the time and date settings of your ZyXEL Device. The updated time is then displayed in the ZyXEL Device error logs.

- 1 Select menu 24 in the main menu to open **Menu 24 – System Maintenance**.
- 2 Then enter 10 to go to **Menu 24.10 – System Maintenance – Time and Date Setting** to update the time and date settings of your ZyXEL Device as shown in the following screen.

**Figure 169** Menu 24.10 System Maintenance: Time and Date Setting

```

Menu 24.10 - System Maintenance - Time and Date Setting

Time Protocol= Manual
Time Server Address= N/A

Current Time:                      00 : 33 : 03
New Time (hh:mm:ss):               00 : 32 : 51

Current Date:                      2000 - 01 - 01
New Date (yyyy-mm-dd):             2000 - 01 - 01

Time Zone= GMT

Daylight Saving= No
Start Date (mm-nth-week-hr):       Jan. - 1st - Sun.(02) - 00
End Date (mm-nth-week-hr):         Jan. - 1st - Sun.(02) - 00

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

**Table 90** System Maintenance: Time and Date Setting

| FIELD               | DESCRIPTION   |
|---------------------|---|
| Time Protocol       | Enter the time service protocol that your time server sends when you turn on the ZyXEL Device. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format.<br><b>Daytime (RFC 867)</b> format is day/month/year/time zone of the server.<br><b>Time (RFC-868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.<br><b>NTP (RFC-1305)</b> is similar to <b>Time (RFC-868)</b> .<br><b>Manual</b> . The default, enter the time manually. |
| Time Server Address | Enter the IP address or domain name of your time server. Check with your ISP/ network administrator if you are unsure of this information.  |
| Current Time        | This field displays an updated time only when you reenter this menu.  |

**Table 90** System Maintenance: Time and Date Setting

| FIELD   | DESCRIPTION   |
|---|---|
| New Time  | Enter the new time in hour, minute and second format.   |
| Current Date  | This field displays an updated date only when you re-enter this menu.   |
| New Date  | Enter the new date in year, month and day format.   |
| Time Zone   | Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).   |
| Daylight Saving   | If you use daylight savings time, then choose <b>Yes</b> .  |
| Start Date  | <p>Configure the day and time when Daylight Saving Time starts if you selected <b>Yes</b> in the <b>Daylight Saving</b> field. The <b>hr</b> field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>Second, Sunday, March</b> and <b>2:00</b>.</p> <p>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Mar., Last, Sun.</b> The time you type in the <b>hr</b> field depends on your time zone. In Germany for instance, you would type 02 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p> |
| End Date  | <p>Configure the day and time when Daylight Saving Time ends if you selected <b>Yes</b> in the <b>Daylight Saving</b> field. The <b>hr</b> field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>First, Sunday, November</b> and <b>2:00</b>.</p> <p>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Oct., Last, Sun.</b> The time you type in the <b>hr</b> field depends on your time zone. In Germany for instance, you would type 02 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>                 |
| Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel. |   |

## 24.2.1 Resetting the Time

The ZyXEL Device resets the time in three instances:

- 1 On leaving menu 24.10 after making changes.
- 2 When the ZyXEL Device starts up, if there is a timeserver configured in menu 24.10.
- 3 24-hour intervals after starting.

## 24.3 Remote Management Setup

### 24.3.1 Telnet

You can configure your ZyXEL Device for remote Telnet access.

### 24.3.2 FTP

You can upload and download ZyXEL Device firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

### 24.3.3 Web

You can use the ZyXEL Device's embedded web configurator for configuration and file management. See the online help for details.

### 24.3.4 Remote Management Setup

Remote management setup is for managing Telnet, FTP and Web services. You can customize the service port, access interface and the secured client IP address to enhance security and flexibility.

You can manage your ZyXEL Device from a remote location via:

The **WLAN only**, the **LAN only**, **All** (LAN and WLAN) or **Disable** (neither).



If you enable remote management of a service, but have applied a filter to block the service, then you will not be able to remotely manage the service.

Enter "11" from menu 24, to display **Menu 24.11 - Remote Management Control** (shown next)

**Figure 170** Menu 24.11 Remote Management Control

| Menu 24.11 - Remote Management Control   |   |              |
|--|---|--------------|
| TELNET Server:                           | Port = 23                                     | Access = ALL |
|  | Secure Client IP = 0.0.0.0                    |              |
| FTP Server:                              | Port = 21                                     | Access = ALL |
|  | Secure Client IP = 0.0.0.0                    |              |
| SSH Server                               | Certificate = auto_generated_self-signed-cert |              |
|  | Port = 22                                     | Access = ALL |
|  | Secure Client IP = 0.0.0.0                    |              |
| HTTPS Server:                            | Certificate = auto_generated_self_signed_cert |              |
|  | Authenticate Client Certificates = No         |              |
|  | Port = 443                                    | Access = ALL |
|  | Secure Client IP = 0.0.0.0                    |              |
| HTTP Server:                             | Port = 80                                     | Access = ALL |
|  | Secure Client IP = 0.0.0.0                    |              |
| SNMP Service:                            | Port = 161                                    | Access = ALL |
|  | Secure Client IP = 0.0.0.0                    |              |
| DNS Service:                             | Port = 53                                     | Access = ALL |
|  | Secure Client IP = 0.0.0.0                    |              |
| Press ENTER to Confirm or ESC to Cancel: |   |              |

The following table describes the fields in this menu.

**Table 91** Menu 24.11 Remote Management Control

| FIELD  | DESCRIPTION   |
|--|---|
| TELNET Server:<br>FTP Server:<br>SSH Server:<br>HTTPS Server:<br>HTTP Server:<br>SNMP Service:<br>DNS Service: | Each of these read-only labels denotes a server or service that you may use to remotely manage the ZyXEL Device.  |
| Port   | This field shows the port number for the remote management service. You can change the port number for a service if needed, but you must use the same port number to use that service for remote management.  |
| Access   | Select the access interface (if any) by pressing the [SPACE BAR]. Choices are: <b>LAN only</b> , <b>WAN only</b> , <b>All</b> or <b>Disable</b> . The default is <b>LAN only</b> .  |
| Secured Client IP  | The default 0.0.0.0 allows any client to use this service to remotely manage the ZyXEL Device. Enter an IP address to restrict access to a client with a matching IP address.   |
| Certificate  | This field displays the name used to identify this certificate. The ZyXEL Device has an automatically generated self signed certificate by default. The factory default certificate is common to all ZyXEL Device's that use certificates. You can replace the certificate when you log into the ZyXEL Device (see <a href="#">Chapter 2 on page 41</a> ) or you can use the Certificates configuration screen (see <a href="#">Chapter 14 on page 169</a> ). |
| Authenticate Client Certificates   | Select <b>Yes</b> by pressing [SPACE BAR]. The internal RADIUS server uses one of the certificates listed in the My Certificates screen to authenticate each wireless client. The exact certificate used depends on the certificate information configured on the wireless client.  |
| Once you have filled in this menu, press [ENTER] to save your configuration, or press [ESC] to cancel.         |   |

### 24.3.5 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- 1 You have disabled that service in menu 24.11.
- 2 The IP address in the **Secure Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.
- 3 There is already another remote management session of the same type (Telnet, FTP or Web) running. You may only have one remote management session of the same type running at one time.
- 4 There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.

## 24.4 System Timeout

There is a system timeout of five minutes (300 seconds) for Telnet/web/FTP connections. Your ZyXEL Device will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys studio` has been changed on the command line.



# Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- [Power and Hardware Connections](#)
- [ZyXEL Device Access and Login](#)
- [Internet Access](#)
- [Wireless Router/AP Troubleshooting](#)

## 25.1 Power and Hardware Connections



---

The ZyXEL Device does not turn on.

---

- 1 Make sure you are using the PoE power injector included with the ZyXEL Device.
- 2 Make sure the PoE power injector is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure the power source is turned on.
- 3 Disconnect and re-connect the PoE power injector to the ZyXEL Device.
- 4 If the problem continues, contact the vendor.

## 25.2 ZyXEL Device Access and Login



---

I forgot the IP address for the ZyXEL Device.

---

- 1 The default IP address is **192.168.1.2**.
- 2 If you changed the static IP address and have forgotten it, you have to reset the device to its factory defaults. Contact your vendor.  
If you set the ZyXEL Device to get a dynamically assigned IP address from a DHCP server, check your DHCP server for the IP address assigned to the ZyXEL Device.



---

**I forgot the password.**

---

- 1 The default password is **1234**.
- 2 If this does not work, you have to reset the device to its factory defaults. Contact your vendor.



---

**I cannot see or access the **Login** screen in the web configurator.**

---

- 1 Make sure you are using the correct IP address.
  - The default IP address is 192.168.1.2.
  - If you changed the IP address ([Section 10.3 on page 134](#)), use the new IP address.
  - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the ZyXEL Device](#).
- 2 Check the hardware connections. See the Quick Start Guide.
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See [Section 25.1 on page 257](#).
- 4 Make sure your computer is in the same subnet as the ZyXEL Device. (If you know that there are routers between your computer and the ZyXEL Device, skip this step.)
  - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the ZyXEL Device.
- 5 Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. Contact your vendor.
- 6 If the problem continues, contact the network administrator or vendor, or try the advanced suggestions.

**Advanced Suggestions**

- Try to access the ZyXEL Device using another service, such as Telnet. If you can access the ZyXEL Device, check the remote management settings to find out why the ZyXEL Device does not respond to HTTP.



---

**I can see the **Login** screen, but I cannot log in to the ZyXEL Device.**

---

- 1 Make sure you have entered the user name and password correctly. The default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 2 You cannot log in to the web configurator while someone is using the SMT or Telnet to access the ZyXEL Device. Log out of the ZyXEL Device in the other session, or ask the person who is logged in to log out.
- 3 Disconnect and re-connect the power adaptor or cord to the ZyXEL Device.

- 4 If this does not work, you have to reset the device to its factory defaults. Contact your vendor.




---

I cannot access the SMT.

---

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.




---

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

---

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.

## 25.3 Internet Access




---

I cannot access the Internet.

---

- 1 Check the hardware connections, and make sure the ZyXEL Device is connected to a broadband modem or router that provides Internet access. See the Quick Start Guide.
- 2 Make sure your Internet account is activated and you entered your ISP account information correctly in the broadband modem or router to which the ZyXEL Device is connected. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 3 If you are trying to access the Internet wirelessly, make sure the wireless settings on the wireless client are the same as the settings on the AP.
- 4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 5 If the problem continues, contact your ISP.




---

I cannot access the Internet anymore. I had access to the Internet (with the ZyXEL Device), but my Internet connection is not available anymore.

---

- 1 Check the hardware connections. See the Quick Start Guide.
- 2 Reboot the ZyXEL Device.
- 3 If the problem continues, contact your ISP.



---

The Internet connection is slow or intermittent.

---

- 1 There might be a lot of traffic on the network. If the ZyXEL Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Make sure the ZyXEL Device is installed in a position free of obstructions.
- 3 Check the signal strength. If the signal is weak, try moving your computer closer to the ZyXEL Device (if possible), and look around to see if there are any devices that might be interfering with the wireless network (microwaves, other wireless networks, and so on).
- 4 Reboot the ZyXEL Device.
- 5 If the problem continues, contact the network administrator or vendor, or try the advanced suggestions.

**Advanced Suggestions**

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

## 25.4 Wireless Router/AP Troubleshooting



---

I cannot access the ZyXEL Device or ping any computer from the WLAN.

---

- 1 Make sure the wireless LAN is enabled on the ZyXEL Device
- 2 Make sure the wireless adapter on the wireless client is working properly.
- 3 Make sure the wireless adapter (installed on your computer) is IEEE 802.11 compatible and supports the same wireless standard as the ZyXEL Device.
- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the ZyXEL Device.
- 5 Check that both the ZyXEL Device and your wireless client are using the same wireless and wireless security settings.
- 6 Make sure you allow the ZyXEL Device to be remotely accessed through the WLAN interface. Check your remote management settings.

# Product Specifications

The following tables summarize the ZyXEL Device's hardware and firmware features.

**Table 92** Hardware Specifications

| SPECIFICATION             | DESCRIPTION   |
|---------------------------|---|
| Dimensions                | 256 (W) x 246 (D) x 82 (H) mm   |
| Weight                    | 2000 g  |
| Power                     | PoE draw: 48V 20W at least  |
| Ethernet Port             | Auto-negotiating: 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode.<br>Auto-crossover: Use either crossover or straight-through Ethernet cables. |
| Power over Ethernet (PoE) | IEEE 802.3af compliant.   |
| Antenna Specifications    | Two external antenna connectors (N-Type).   |
| Output Power              | IEEE 802.11b/g: 17 dBm<br>IEEE 802.11a: 14 dBm  |
| Operating Environment     | Temperature: -40° C ~ 60° C<br>Humidity: 10% ~ 90% RH   |

**Table 92** Hardware Specifications

| SPECIFICATION       | DESCRIPTION   |
|---------------------|---|
| Storage Environment | Temperature: -40° C ~ 70° C<br>Humidity: 5% ~ 95% RH  |
| Approvals           | Radio <ul style="list-style-type: none"> <li>• USA:<br/>FCC Part 15C 15.247<br/>FCC Part 15E 15.407<br/>FCC OET65</li> <li>• EU:<br/>ETSI EN 300 328 V1.7.1<br/>ETSI EN 301 893 V1.2.3</li> <li>• Taiwan:<br/>DGT LP0002</li> <li>• Canada:<br/>Industry Canada RSS-210</li> <li>• Australia:<br/>AS/NZS 4268</li></ul> EMC/ EMI <ul style="list-style-type: none"> <li>• USA:<br/>FCC Part 15 Subpart B</li> <li>• EU:<br/>EN 301 489-17 V1.2.1: 08-2002<br/>EN 55022:2006</li> <li>• Canada:<br/>ICES-003</li> <li>• Australia:<br/>AS/NZS CISPR22</li></ul> EMC/ EMS <ul style="list-style-type: none"> <li>• EU:<br/>EN 301 489-1 V1.5.1: 11-2004</li></ul> |

**Table 93** Firmware Specifications

|   |   |
|---|---|
| Default IP Address                              | 192.168.1.2   |
| Default Subnet Mask                             | 255.255.255.0 (24 bits)   |
| Default Password                                | 1234  |
| Wireless LAN Standards                          | IEEE 802.11a, IEEE 802.11b, IEEE 802.11g  |
| Wireless security                               | WEP, WPA(2), WPA(2)-PSK, IEEE 802.1x  |
| Layer 2 isolation                               | Prevents wireless clients associated with your ZyXEL Device from communicating with other wireless clients, APs, computers or routers in a network.   |
| Multiple BSSID (MBSSID)                         | MBSSID mode allows the ZyXEL Device to operate up to 8 different wireless networks (BSSs) simultaneously, each with independently-configurable wireless and security settings.  |
| Rogue AP detection                              | Rogue AP detection detects and logs unknown access points (APs) operating in the area.  |
| Internal RADIUS server                          | PEAP, 32-entry Trusted AP list, 128-entry Trusted Users list.   |
| VLAN  | 802.1Q VLAN tagging.  |
| STP (Spanning Tree Protocol) / RSTP (Rapid STP) | (R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP-compliant bridges in your network to ensure that only one path exists between any two stations on the network. |

**Table 93** Firmware Specifications

|                               |  |
|-------------------------------|--|
| WMM QoS                       | WMM (Wi-Fi MultiMedia) QoS (Quality of Service) allows you to prioritize wireless traffic.   |
| Certificates                  | The ZyXEL Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. Certificates provide a way to exchange public keys for use in authentication.   |
| SSL Passthrough               | SSL (Secure Sockets Layer) uses a public key to encrypt data that's transmitted over an SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https" instead of "http". The ZyXEL Device allows SSL connections to take place through the ZyXEL Device.      |
| MAC Address Filter            | Your ZyXEL Device checks the MAC address of the wireless station against a list of allowed or denied MAC addresses.  |
| Wireless Association List     | With the wireless association list, you can see the list of the wireless stations that are currently using the ZyXEL Device to access your wired network.  |
| Logging and Tracing           | Built-in message logging and packet tracing.   |
| Embedded FTP and TFTP Servers | The embedded FTP and TFTP servers enable fast firmware upgrades as well as configuration file backups and restoration.   |
| Auto Configuration            | Administrators can use text configuration files to configure the wireless LAN settings for multiple APs. The AP can automatically get a configuration file from a TFTP server at start up or after renewing DHCP client information.   |
| SNMP                          | SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyXEL Device supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1) and version two c (SNMPv2c). The NWA-3165 also supports version 3 (SNMPv3). |
| DFS                           | DFS (Dynamic Frequency Selection) allows a wider choice of 802.11a wireless channels.  |

## Compatible ZyXEL Antennas

At the time of writing, you can use the following antennas in your ZyXEL Device.

**Table 94** ZyXEL Device Compatible Antennas

| MODEL<br>FEATURES           | EXT-108       | EXR-109       | EXT-114       | EXT-118       | ANT2206      |             | ANT3108       | ANT3218       |
|-----------------------------|---------------|---------------|---------------|---------------|--------------|-------------|---------------|---------------|
| Frequency Band (MHz)        | 2400 ~ 2500   | 2400 ~ 2500   | 2400 ~ 2500   | 2400 ~ 2500   | 2400 ~ 2500  | 4900 ~ 5875 | 5150 ~ 5875   | 4900 ~ 5875   |
| Gain (dBi)                  | 8             | 9             | 14            | 18            | 6            | 8           | 8             | 18            |
| Max. VSWR                   | 2.0:1         | 1.5:1         | 1.5:1         | 1.5:1         | 2.0:1        | 2.0:1       | 2.0:1         | 2.0:1         |
| HPBW/<br>Horizontal         | 360°          | 65°           | 30°           | 15°           | 65°          | 50°         | 360°          | 18°           |
| HPBW/<br>Vertical           | 15°           | 60°           | 30°           | 5°            | 75°          | 50°         | 20°           | 18°           |
| Impedance (Ohm)             | 50            | 50            | 50            | 50            | 50           |             | 50            | 50            |
| Connector                   | N type female | N type female | N type female | N type female | RP SMA plug  |             | N type female | N type female |
| Survival Wind Speed (km/hr) | 216           | 216           | 216           | 180           |              |             | 216           | 216           |
| Temperature                 | -40°C ~ 80°C  | -40°C ~ 80°C  | -40°C ~ 80°C  | -40°C ~ 80°C  | -10°C ~ 55°C |             | -40°C ~ 80°C  | -40°C ~ 80°C  |
| Humidity                    | 95% at 25°C   | 95% at 55°C   | 95% at 55°C   | 95% at 55°C   | 95% at 55°C  |             | 95% at 55°C   | 95% at 55°C   |
| Weight                      | 337 gw        | 107 gw        | 407 g         | 1.6 kg        | 110 g        |             | 206 g         | 640 gw        |

## Compatible ZyXEL Antenna Cables

The following table shows you the cables you can use in the ZyXEL Device to extend your connection to antennas at the time of writing.

**Table 95** ZyXEL Device Compatible Antenna Cables

| MODEL NAME | PART NUMBER (P/N) | LENGTH                        |
|------------|-------------------|-------------------------------|
| LMR-400    | 91-005-075001G    | N-PLUG to N-PLUG, for 6M      |
|            | 91-005-075002G    | N-PLUG to N-PLUG, for 9M      |
|            | 91-005-075003G    | N-PLUG to N-PLUG, for 12M     |
|            | 91-005-075004G    | N-PLUG to N-PLUG, for 1M      |
| LMR-200    | 91-005-074001G    | N-PLUG to RP-SMA PLUG, for 3M |
|            | 91-005-074002G    | N-PLUG to RP-SMA PLUG, for 6M |
|            | 91-005-074003G    | N-PLUG to RP-SMA PLUG, for 9M |
| EXT-300    | 91-005-082001B    | Jumper Cable, Surge Arrstor   |

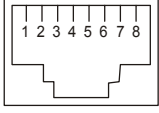
## Power over Ethernet (PoE) Specifications

You can use a power over Ethernet injector to power this device. The injector must comply to IEEE 802.3af.

**Table 96** Power over Ethernet Injector Specifications

|               |                    |
|---------------|--------------------|
| Power Output  | 15.4 Watts maximum |
| Power Current | 400 mA maximum     |

**Table 97** Power over Ethernet Injector RJ-45 Port Pin Assignments

|  | PIN NO | RJ-45 SIGNAL ASSIGNMENT |
|---|--------|-------------------------|
|   | 1      | Output Transmit Data +  |
|   | 2      | Output Transmit Data -  |
|   | 3      | Receive Data +          |
|   | 4      | Power +                 |
|   | 5      | Power +                 |
|   | 6      | Receive Data -          |
|   | 7      | Power -                 |
|   | 8      | Power -                 |



---

# PART IV

## Appendices and Index

---

Setting up Your Computer's IP Address (269)  
Wireless LANs (281)  
Pop-up Windows, JavaScripts and Java Permissions (295)  
IP Addresses and Subnetting (301)  
Text File Based Auto Configuration (309)  
Legal Information (317)  
Customer Support (321)  
Index (327)



# Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

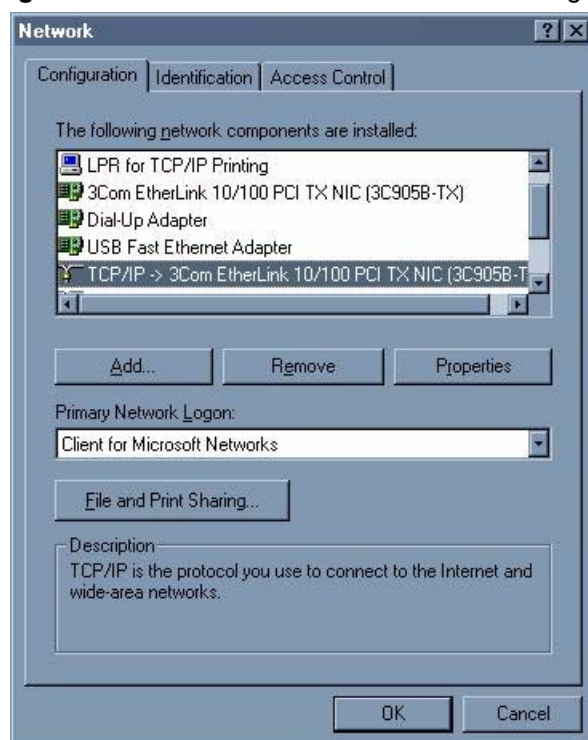
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the ZyXEL Device's LAN port.

## Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window

**Figure 171** Windows 95/98/Me: Network: Configuration

## Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- 1 In the **Network** window, click **Add**.
- 2 Select **Adapter** and then click **Add**.
- 3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- 1 In the **Network** window, click **Add**.
- 2 Select **Protocol** and then click **Add**.
- 3 Select **Microsoft** from the list of **manufacturers**.
- 4 Select **TCP/IP** from the list of network protocols and then click **OK**.

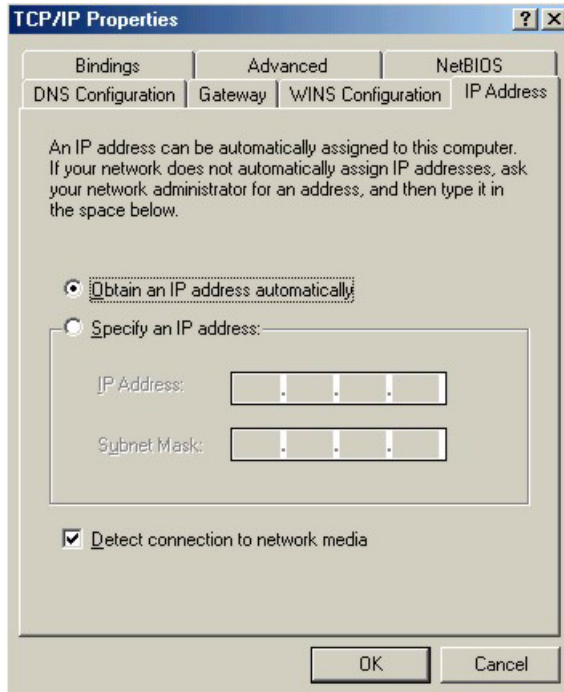
If you need Client for Microsoft Networks:

- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.
- 3 Select **Microsoft** from the list of manufacturers.
- 4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- 5 Restart your computer so the changes you made take effect.

## Configuring

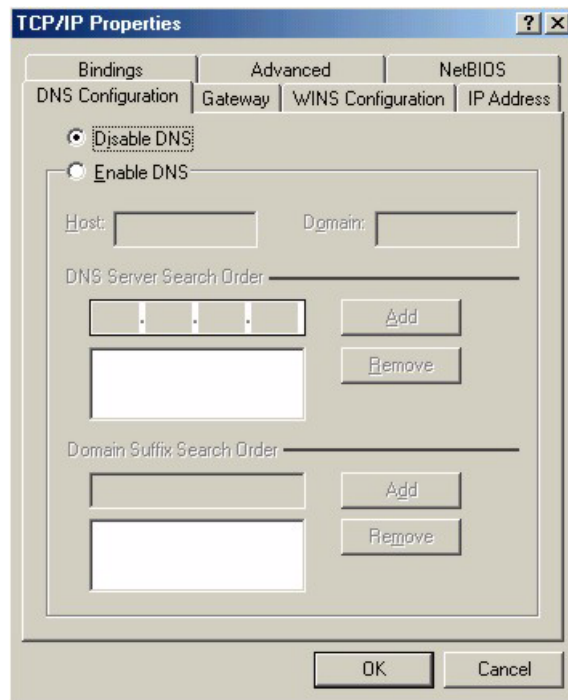
- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the **IP Address** tab.
  - If your IP address is dynamic, select **Obtain an IP address automatically**.
  - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

**Figure 172** Windows 95/98/Me: TCP/IP Properties: IP Address



- 3 Click the **DNS Configuration** tab.
  - If you do not know your DNS information, select **Disable DNS**.
  - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

**Figure 173** Windows 95/98/Me: TCP/IP Properties: DNS Configuration



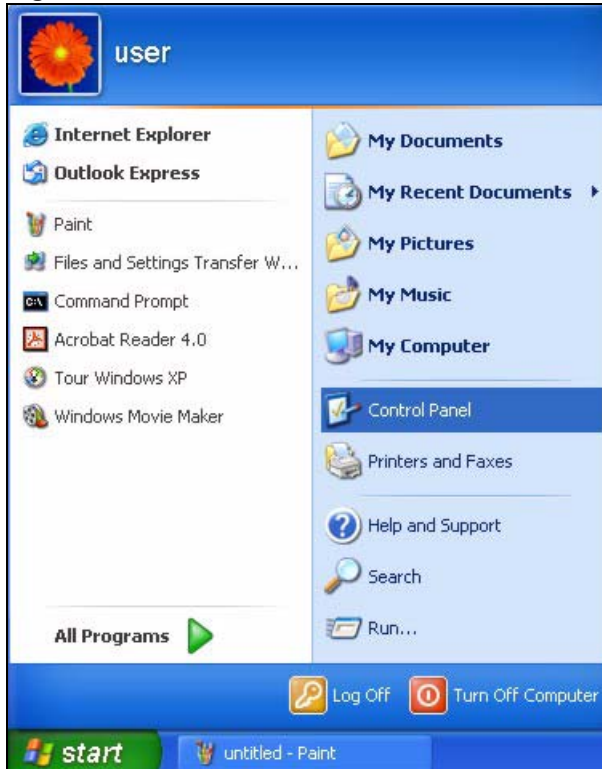
- 4 Click the **Gateway** tab.
  - If you do not know your gateway's IP address, remove previously installed gateways.
  - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
- 5 Click **OK** to save and close the **TCP/IP Properties** window.
- 6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
- 7 Turn on your ZyXEL Device and restart your computer when prompted.

## Verifying Settings

- 1 Click **Start** and then **Run**.
- 2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
- 3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

## Windows 2000/NT/XP

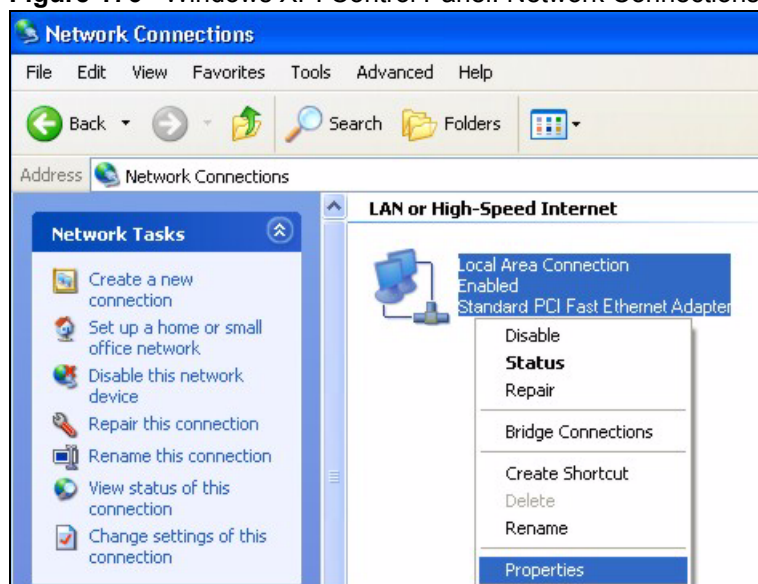
- 1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

**Figure 174** Windows XP: Start Menu

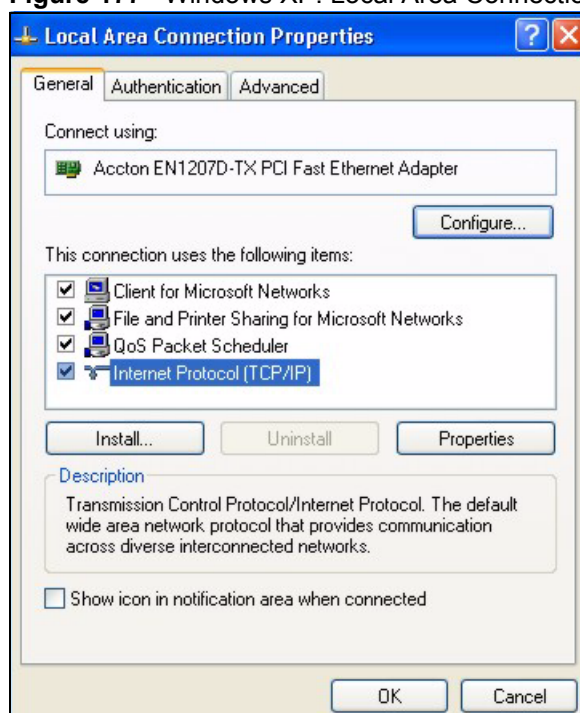
- 2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

**Figure 175** Windows XP: Control Panel

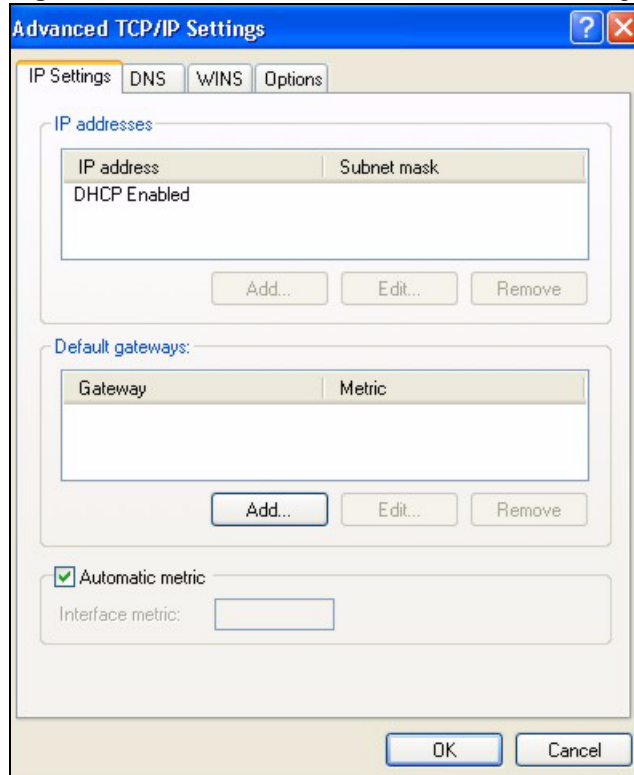
- 3 Right-click **Local Area Connection** and then click **Properties**.

**Figure 176** Windows XP: Control Panel: Network Connections: Properties

- 4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

**Figure 177** Windows XP: Local Area Connection Properties

- 5 The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).
  - If you have a dynamic IP address click **Obtain an IP address automatically**.
  - If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. Click **Advanced**.

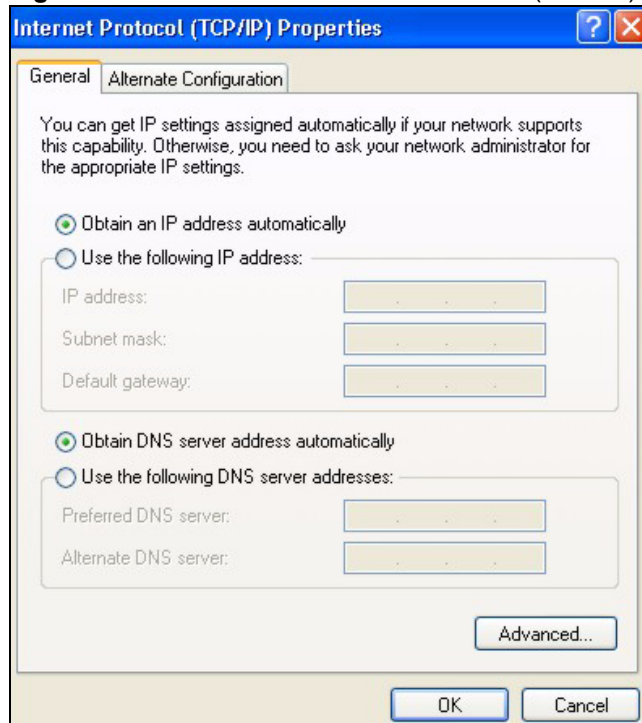
**Figure 178** Windows XP: Advanced TCP/IP Settings

- 6** If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
  - In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
  - Repeat the above two steps for each IP address you want to add.
  - Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
  - In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
  - Click **Add**.
  - Repeat the previous three steps for each default gateway you want to add.
  - Click **OK** when finished.
- 7** In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):
- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
  - If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.
- If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 179** Windows XP: Internet Protocol (TCP/IP) Properties



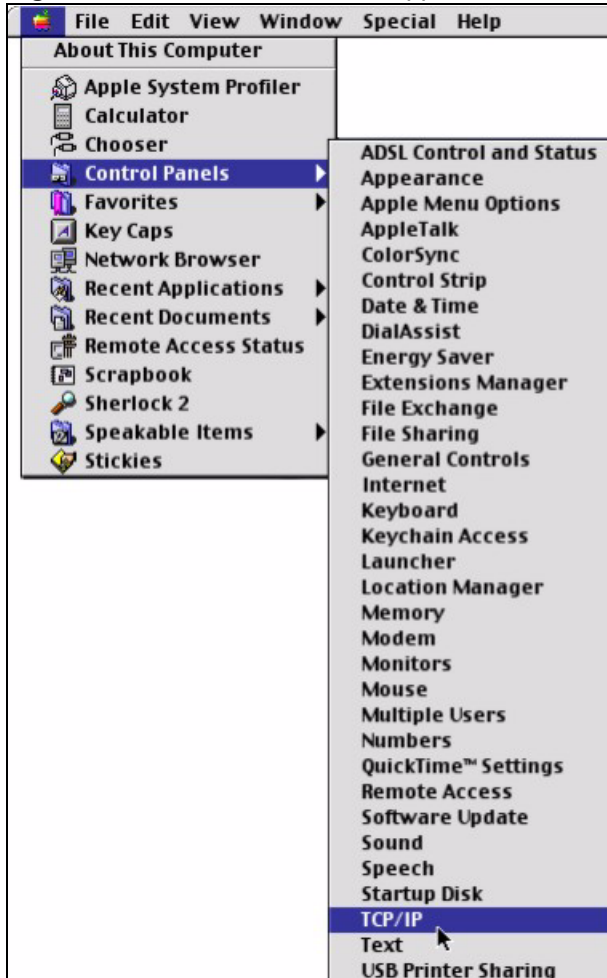
- 8** Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9** Click **OK** to close the **Local Area Connection Properties** window.
- 10** Turn on your ZyXEL Device and restart your computer (if prompted).

## Verifying Settings

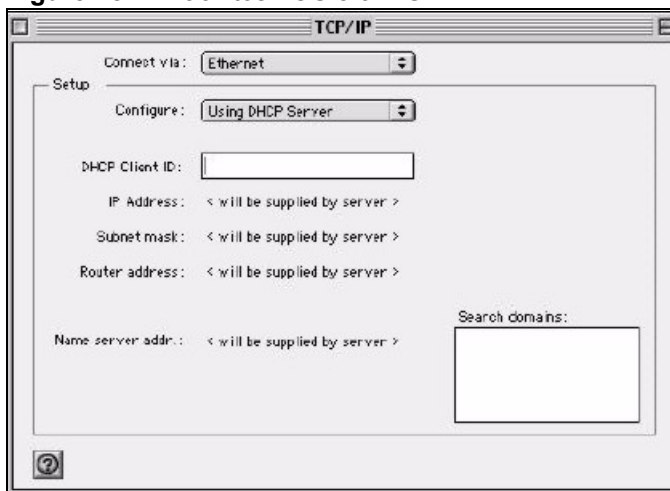
- 1** Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.
- 2** In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Macintosh OS 8/9

- 1** Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

**Figure 180** Macintosh OS 8/9: Apple Menu

2 Select **Ethernet built-in** from the **Connect via** list.

**Figure 181** Macintosh OS 8/9: TCP/IP

3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.

- Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your ZyXEL Device in the **Router address** box.
- 5** Close the **TCP/IP Control Panel**.
  - 6** Click **Save** if prompted, to save changes to your configuration.
  - 7** Turn on your ZyXEL Device and restart your computer (if prompted).

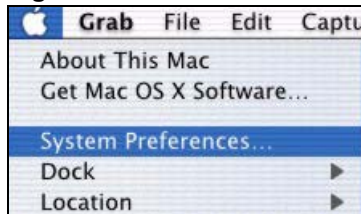
## Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

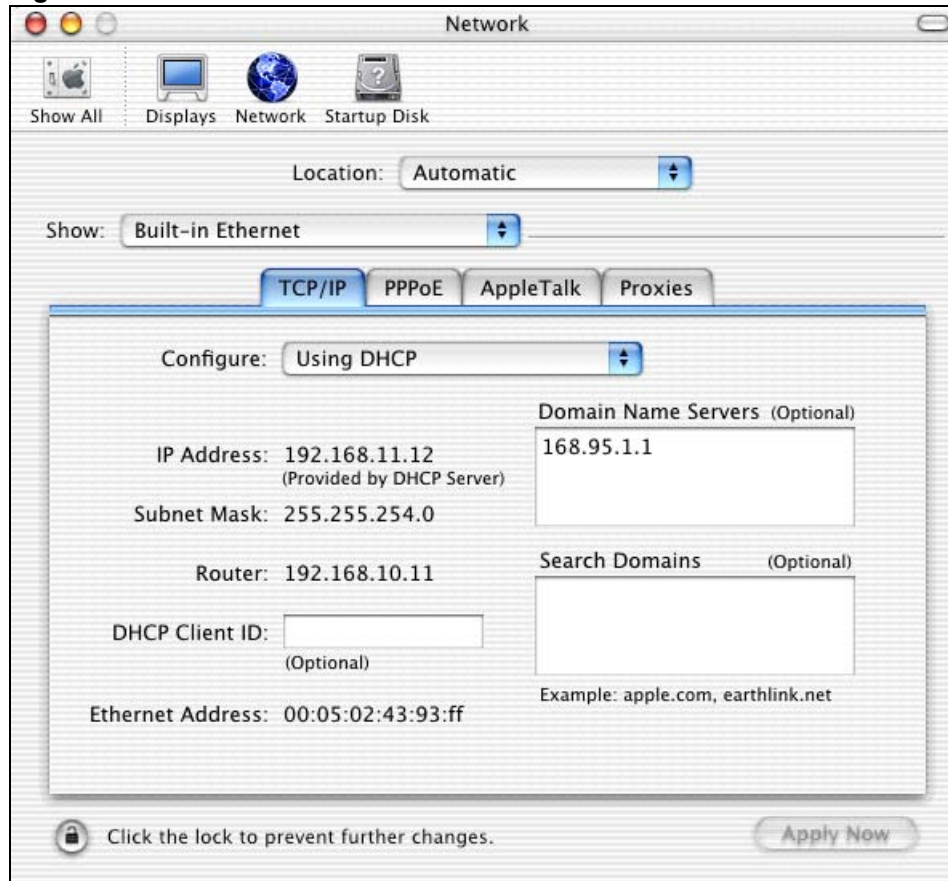
## Macintosh OS X

- 1** Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

**Figure 182** Macintosh OS X: Apple Menu



- 2** Click **Network** in the icon bar.
  - Select **Automatic** from the **Location** list.
  - Select **Built-in Ethernet** from the **Show** list.
  - Click the **TCP/IP** tab.
- 3** For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

**Figure 183** Macintosh OS X: Network

- 4 For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your ZyXEL Device in the **Router address** box.
- 5 Click **Apply Now** and close the window.
- 6 Turn on your ZyXEL Device and restart your computer (if prompted).

## Verifying Settings

Check your TCP/IP properties in the **Network** window.



# Wireless LANs

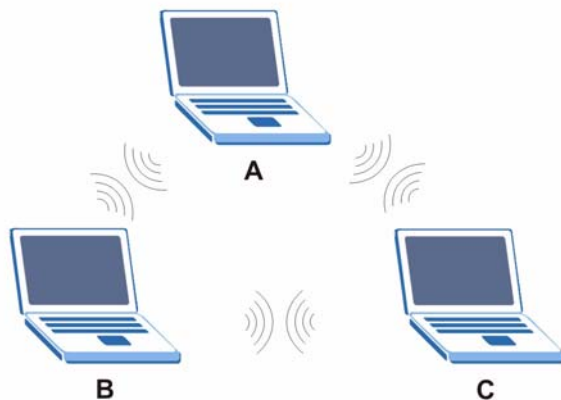
## Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

### Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

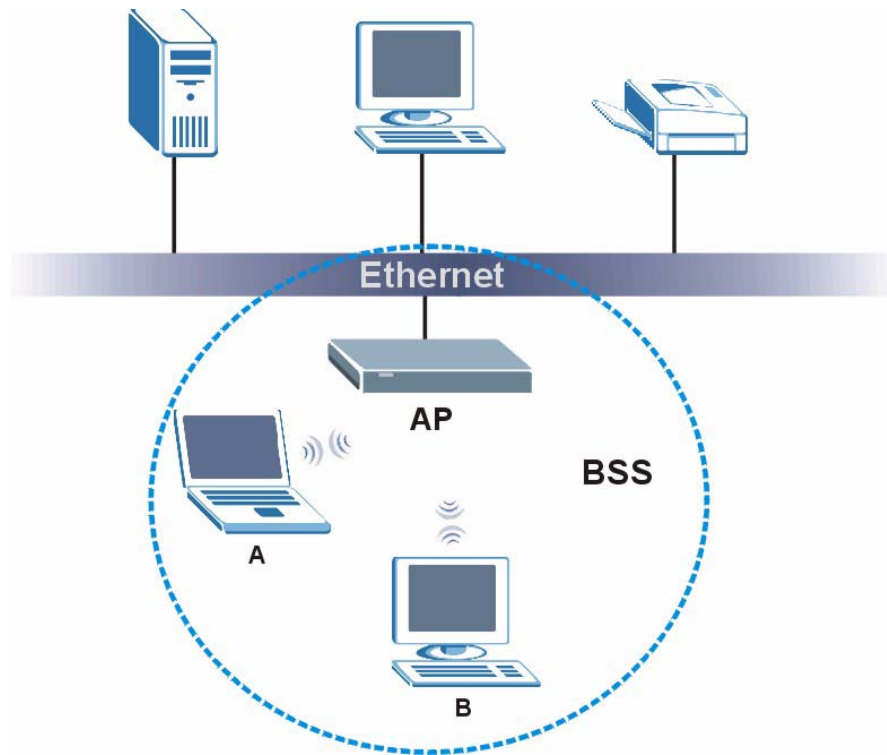
**Figure 184** Peer-to-Peer Communication in an Ad-hoc Network



### BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

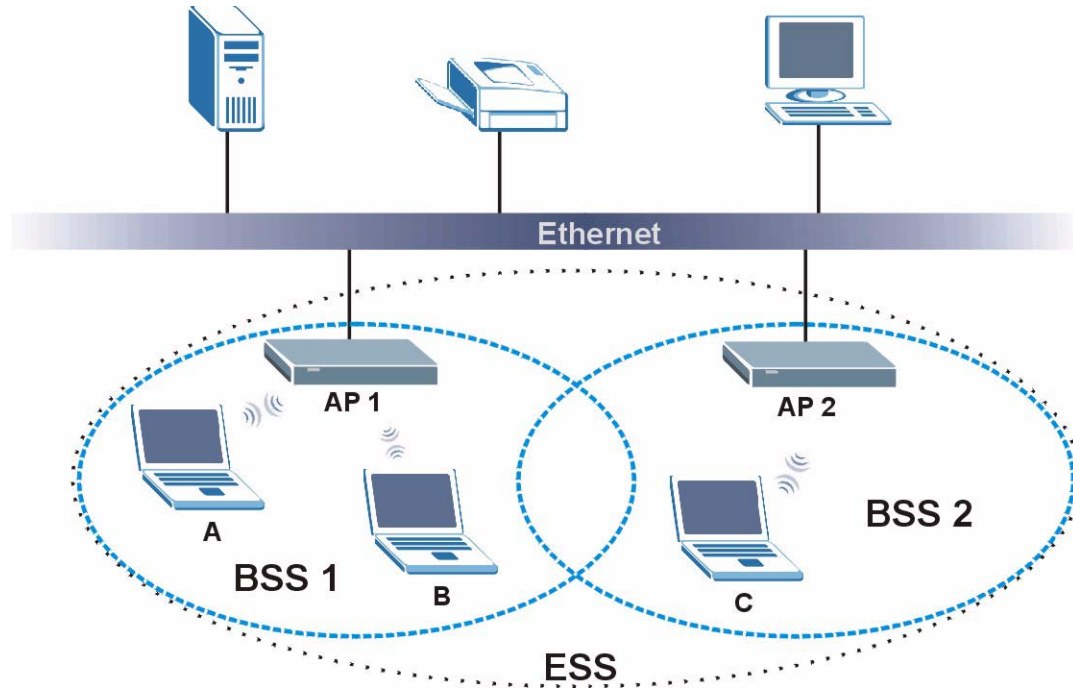
**Figure 185** Basic Service Set

## ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

**Figure 186** Infrastructure WLAN

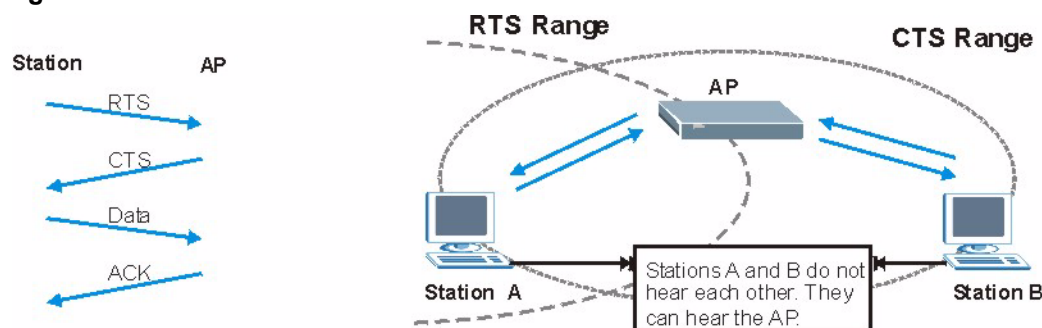
## Channel

A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

## RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

**Figure 187** RTS/CTS

When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

**RTS/CTS** is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.



Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

## Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

## Preamble Type

Preamble is used to signal that data is coming to the receiver. **Short** and **Long** refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b/g compliant wireless adapters support long preamble, but not all support short preamble.

Select **Long** preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.

Select **Short** preamble if you are sure the wireless adapters support it, and to provide more efficient communications.

Select **Dynamic** to have the AP automatically use short preamble when wireless adapters support it, otherwise the AP uses long preamble.



The AP and the wireless adapters **MUST** use the same preamble mode in order to communicate.

## IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

**Table 98** IEEE 802.11g

| DATA RATE (MBPS)      | MODULATION   |
|-----------------------|--|
| 1                     | DBPSK (Differential Binary Phase Shift Keyed)      |
| 2                     | DQPSK (Differential Quadrature Phase Shift Keying) |
| 5.5 / 11              | CCK (Complementary Code Keying)                    |
| 6/9/12/18/24/36/48/54 | OFDM (Orthogonal Frequency Division Multiplexing)  |

## Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the ZyXEL Device are data encryption, wireless client authentication, restricting access by device MAC address and hiding the ZyXEL Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your ZyXEL Device.

**Table 99** Wireless Security Levels

| SECURITY LEVEL | SECURITY TYPE                                    |
|----------------|--|
| Least Secure   | Unique SSID (Default)                            |
|                | Unique SSID with Hide SSID Enabled               |
|                | MAC Address Filtering                            |
|                | WEP Encryption                                   |
|                | IEEE802.1x EAP with RADIUS Server Authentication |
|                | Wi-Fi Protected Access (WPA)                     |
| Most Secure    | WPA2   |



---

You must enable the same wireless security settings on the ZyXEL Device and on all wireless clients that you want to associate with it.

---

## IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

## RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication
  - Determines the identity of the users.
- Authorization

Determines the network services available to authenticated users once they are connected to the network.

- Accounting  
Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

## Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request  
Sent by an access point requesting authentication.
- Access-Reject  
Sent by a RADIUS server rejecting access.
- Access-Accept  
Sent by a RADIUS server allowing access.
- Access-Challenge  
Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request  
Sent by the access point requesting accounting.
- Accounting-Response  
Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

## Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

### **EAP-MD5 (Message-Digest Algorithm 5)**

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client ‘proves’ that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

### **EAP-TLS (Transport Layer Security)**

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender’s identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

### **EAP-TTLS (Tunneled Transport Layer Service)**

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

### **PEAP (Protected EAP)**

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

### **LEAP**

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

## Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.



### EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

**Table 100** Comparison of EAP Authentication Types

|                            | EAP-MD5 | EAP-TLS | EAP-TTLS | PEAP     | LEAP     |
|----------------------------|---------|---------|----------|----------|----------|
| Mutual Authentication      | No      | Yes     | Yes      | Yes      | Yes      |
| Certificate – Client       | No      | Yes     | Optional | Optional | No       |
| Certificate – Server       | No      | Yes     | Yes      | Yes      | No       |
| Dynamic Key Exchange       | No      | Yes     | Yes      | Yes      | Yes      |
| Credential Integrity       | None    | Strong  | Strong   | Strong   | Moderate |
| Deployment Difficulty      | Easy    | Hard    | Moderate | Moderate | Moderate |
| Client Identity Protection | No      | No      | Yes      | Yes      | No       |

## WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

## Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevents all wireless devices sharing the same encryption keys. (a weakness of WEP)

## User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

## Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

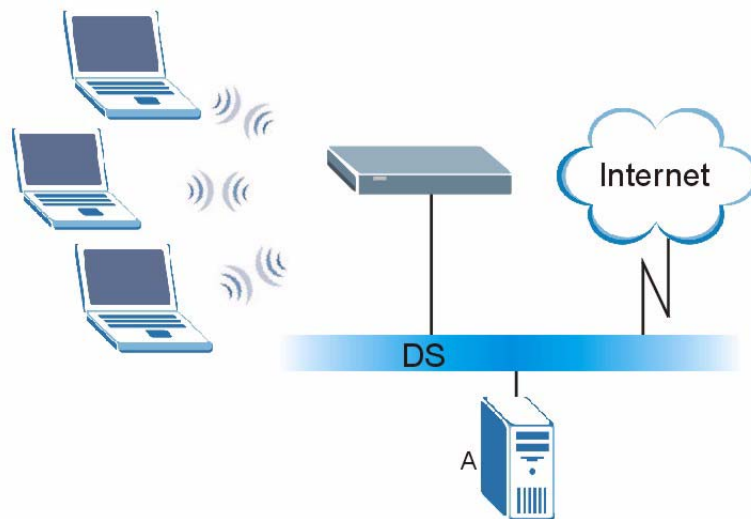
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

## WPA(2) with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

- 1 The AP passes the wireless client's authentication request to the RADIUS server.
- 2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3 The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

**Figure 188** WPA(2) with RADIUS Application Example



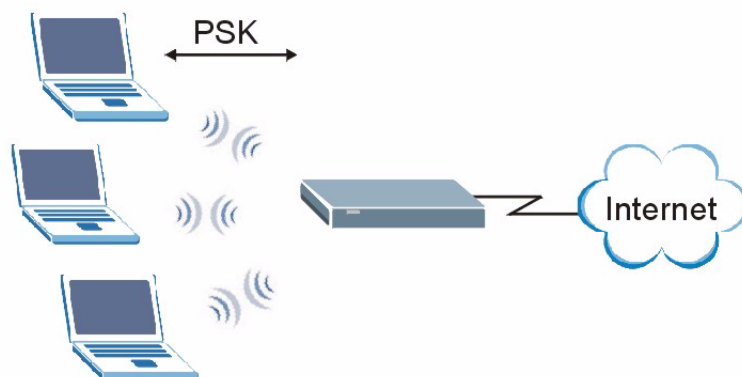
## WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

- 1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
- 2 The AP checks each wireless client's password and (only) allows it to join the network if the password matches.
- 3 The AP and wireless clients use the pre-shared key to generate a common PMK (Pairwise Master Key).

- 4 The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

**Figure 189** WPA(2)-PSK Authentication



## Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

**Table 101** Wireless Security Relational Matrix

| AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL | ENCRYPTION METHOD | ENTER MANUAL KEY | IEEE 802.1X                    |
|--|-------------------|------------------|--------------------------------|
| Open   | None              | No               | Disable                        |
|  |                   |                  | Enable without Dynamic WEP Key |
| Open   | WEP               | No               | Enable with Dynamic WEP Key    |
|  |                   | Yes              | Enable without Dynamic WEP Key |
|  |                   | Yes              | Disable                        |
| Shared   | WEP               | No               | Enable with Dynamic WEP Key    |
|  |                   | Yes              | Enable without Dynamic WEP Key |
|  |                   | Yes              | Disable                        |
| WPA  | TKIP/AES          | No               | Enable                         |
| WPA-PSK  | TKIP/AES          | Yes              | Disable                        |
| WPA2   | TKIP/AES          | No               | Enable                         |
| WPA2-PSK                                       | TKIP/AES          | Yes              | Disable                        |

## Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

## Antenna Characteristics

### Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b) or 5GHz(IEEE 802.11a) is needed to communicate efficiently in a wireless LAN.

### Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

### Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

## Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

## Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to-point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

# Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).



Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

## Internet Explorer Pop-up Blockers

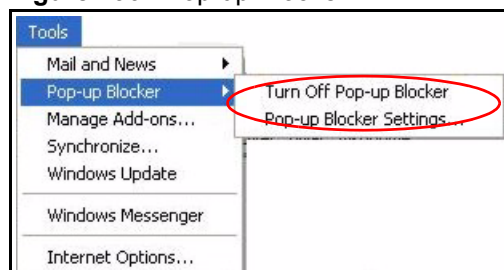
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

### Disable pop-up Blockers

- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

**Figure 190** Pop-up Blocker

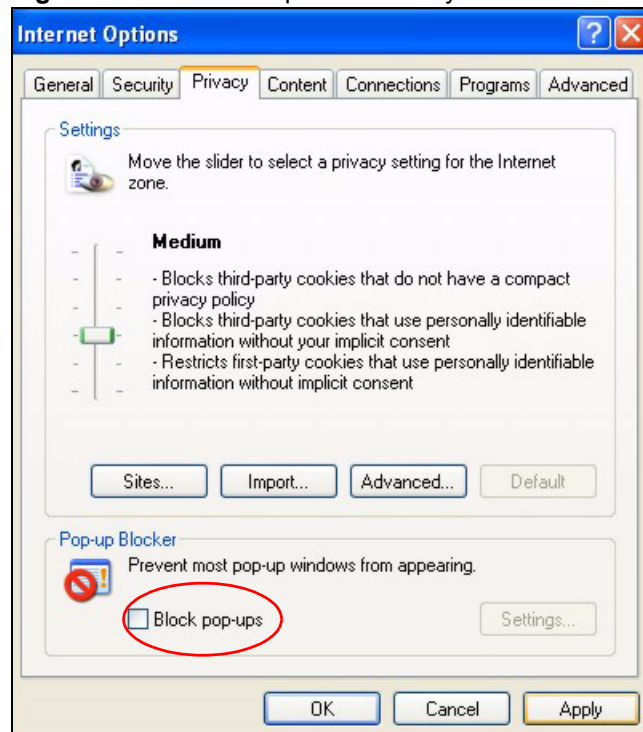


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.

- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

**Figure 191** Internet Options: Privacy

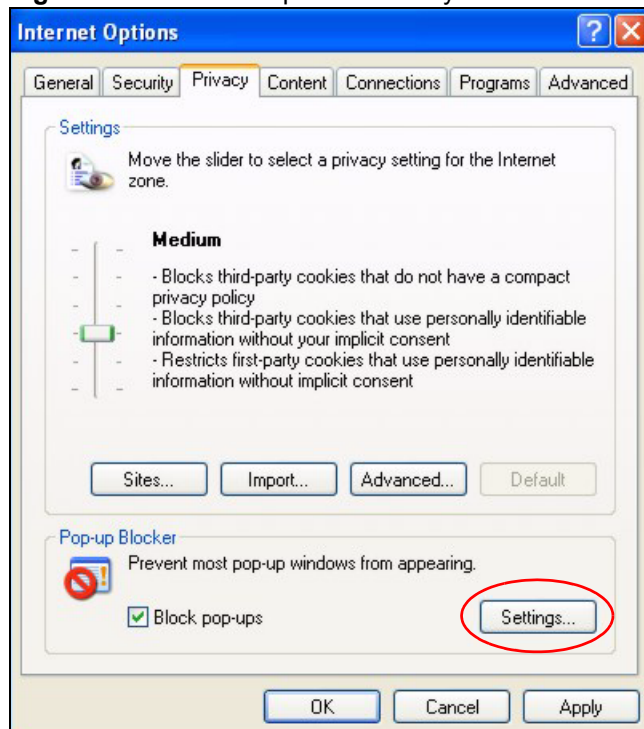


- 3 Click **Apply** to save this setting.

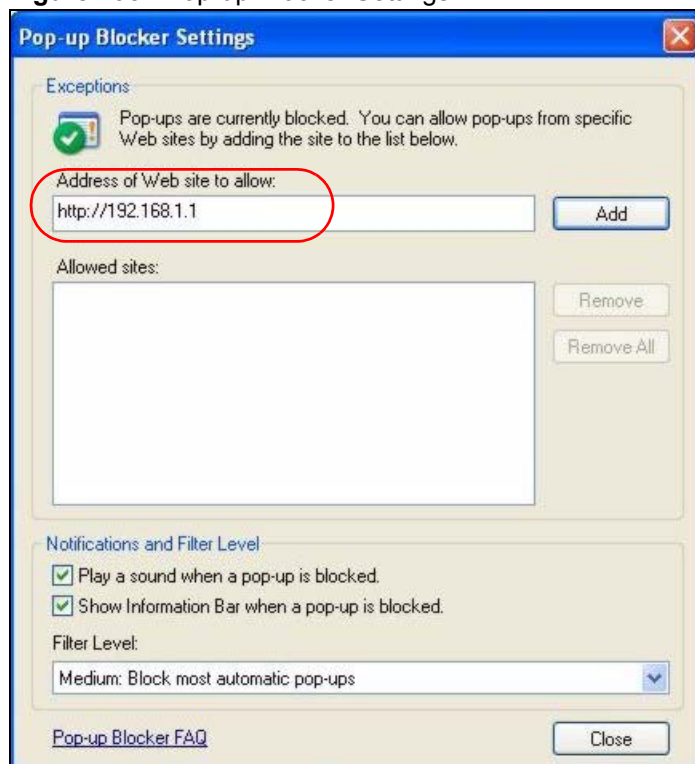
## Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1 In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.
- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

**Figure 192** Internet Options: Privacy

- 3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.
- 4 Click **Add** to move the IP address to the list of **Allowed sites**.

**Figure 193** Pop-up Blocker Settings

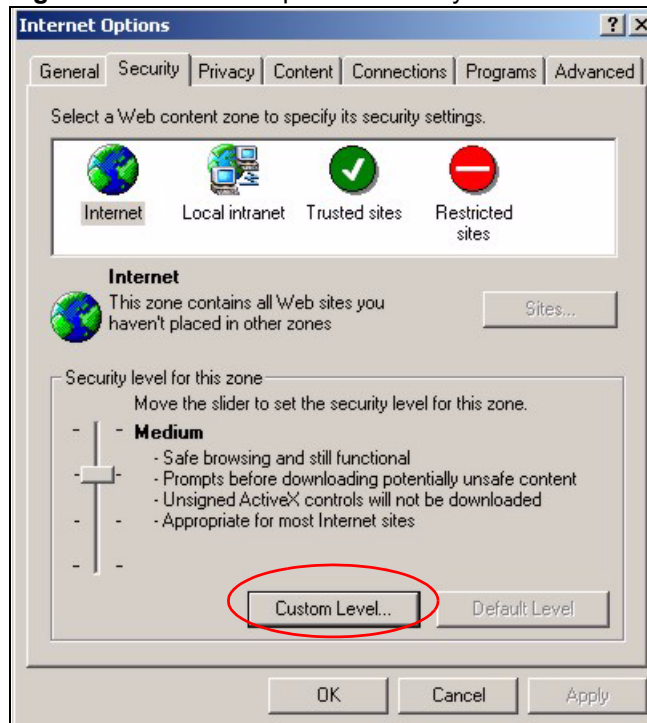
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

## JavaScripts

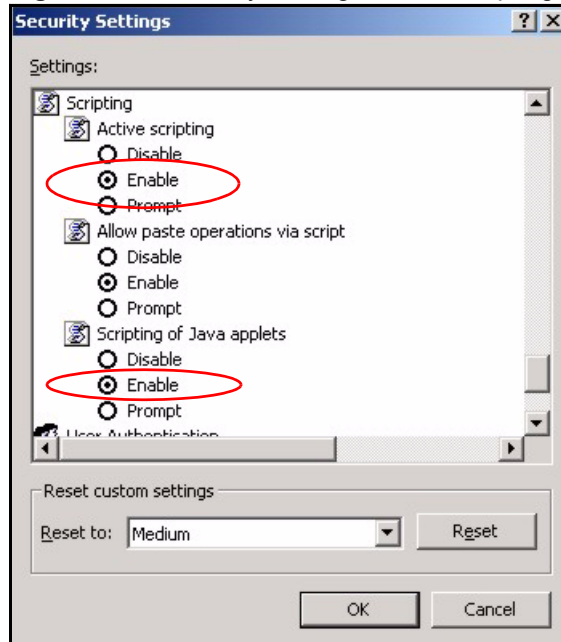
If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

- 1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

**Figure 194** Internet Options: Security

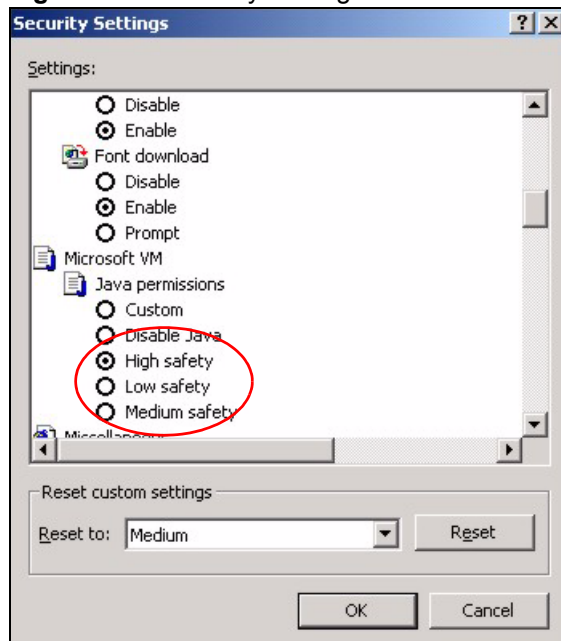


- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
- 6 Click **OK** to close the window.

**Figure 195** Security Settings - Java Scripting

## Java Permissions

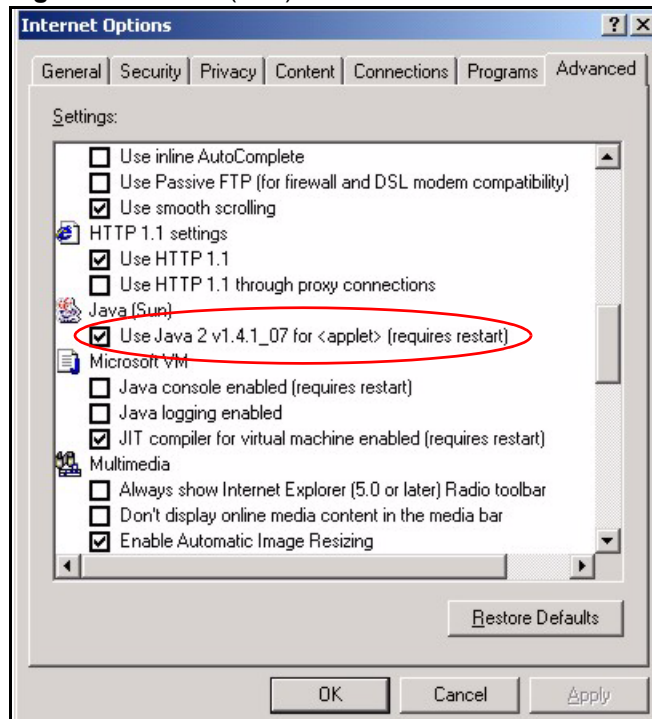
- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.
- 5 Click **OK** to close the window.

**Figure 196** Security Settings - Java

## JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
- 3 Click **OK** to close the window.

**Figure 197** Java (Sun)



# IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

## Introduction to IP Addresses

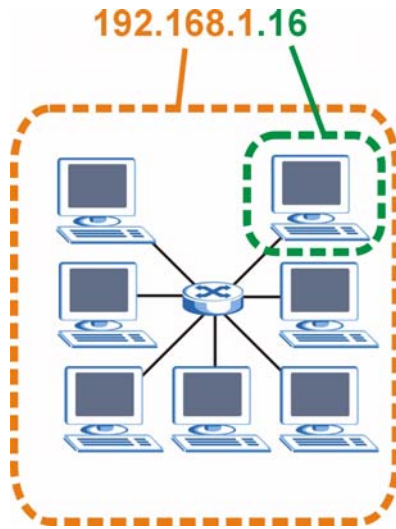
One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

## Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

**Figure 198** Network Number and Host ID

How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

**Table 102** Subnet Masks

|                      | <b>1ST OCTET:<br/>(192)</b> | <b>2ND<br/>OCTET:<br/>(168)</b> | <b>3RD<br/>OCTET:<br/>(1)</b> | <b>4TH OCTET<br/>(2)</b> |
|----------------------|-----------------------------|---------------------------------|-------------------------------|--------------------------|
| IP Address (Binary)  | 11000000                    | 10101000                        | 00000001                      | 00000010                 |
| Subnet Mask (Binary) | <b>11111111</b>             | <b>11111111</b>                 | <b>11111111</b>               | 00000000                 |
| Network Number       | <b>11000000</b>             | <b>10101000</b>                 | <b>00000001</b>               |                          |
| Host ID              |                             |                                 |                               | 00000010                 |

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

**Table 103** Subnet Masks

|             | BINARY    |           |           |           | DECIMAL         |
|-------------|-----------|-----------|-----------|-----------|-----------------|
|             | 1ST OCTET | 2ND OCTET | 3RD OCTET | 4TH OCTET |                 |
| 8-bit mask  | 11111111  | 00000000  | 00000000  | 00000000  | 255.0.0.0       |
| 16-bit mask | 11111111  | 11111111  | 00000000  | 00000000  | 255.255.0.0     |
| 24-bit mask | 11111111  | 11111111  | 11111111  | 00000000  | 255.255.255.0   |
| 29-bit mask | 11111111  | 11111111  | 11111111  | 11111000  | 255.255.255.248 |

## Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

**Table 104** Maximum Host Numbers

| SUBNET MASK |                 | HOST ID SIZE |              | MAXIMUM NUMBER OF HOSTS |
|-------------|-----------------|--------------|--------------|-------------------------|
| 8 bits      | 255.0.0.0       | 24 bits      | $2^{24} - 2$ | 16777214                |
| 16 bits     | 255.255.0.0     | 16 bits      | $2^{16} - 2$ | 65534                   |
| 24 bits     | 255.255.255.0   | 8 bits       | $2^8 - 2$    | 254                     |
| 29 bits     | 255.255.255.248 | 3 bits       | $2^3 - 2$    | 6                       |

## Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

**Table 105** Alternative Subnet Mask Notation

| SUBNET MASK     | ALTERNATIVE NOTATION | LAST OCTET (BINARY) | LAST OCTET (DECIMAL) |
|-----------------|----------------------|---------------------|----------------------|
| 255.255.255.0   | /24                  | 0000 0000           | 0                    |
| 255.255.255.128 | /25                  | 1000 0000           | 128                  |

**Table 105** Alternative Subnet Mask Notation (continued)

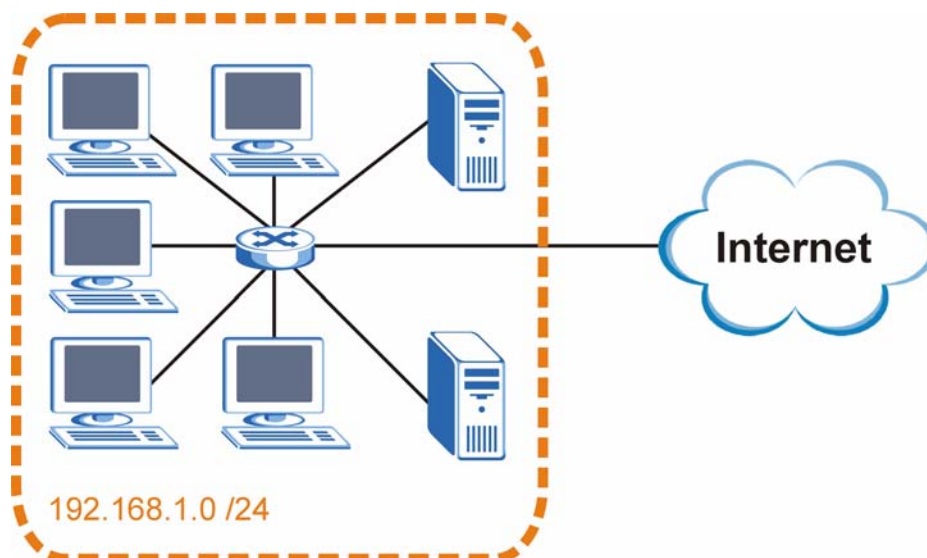
| SUBNET MASK     | ALTERNATIVE NOTATION | LAST OCTET (BINARY) | LAST OCTET (DECIMAL) |
|-----------------|----------------------|---------------------|----------------------|
| 255.255.255.192 | /26                  | 1100 0000           | 192                  |
| 255.255.255.224 | /27                  | 1110 0000           | 224                  |
| 255.255.255.240 | /28                  | 1111 0000           | 240                  |
| 255.255.255.248 | /29                  | 1111 1000           | 248                  |
| 255.255.255.252 | /30                  | 1111 1100           | 252                  |

## Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of  $2^8 - 2$  or 254 possible hosts.

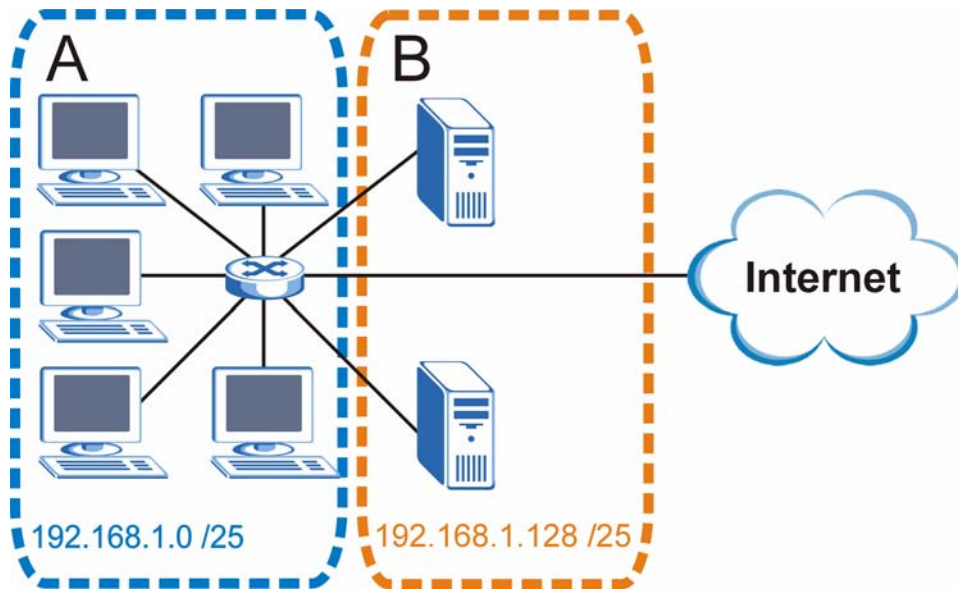
The following figure shows the company network before subnetting.

**Figure 199** Subnetting Example: Before Subnetting

You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

**Figure 200** Subnetting Example: After Subnetting

In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of  $2^7 - 2$  or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

## Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to “borrow” two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving  $2^6 - 2$  or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

**Table 106** Subnet 1

| IP/SUBNET MASK                     | NETWORK NUMBER                | LAST OCTET BIT VALUE |
|------------------------------------|-------------------------------|----------------------|
| IP Address (Decimal)               | 192.168.1.                    | 0                    |
| IP Address (Binary)                | 11000000.10101000.00000001.   | 00000000             |
| Subnet Mask (Binary)               | 11111111.11111111.11111111.   | 11000000             |
| Subnet Address:<br>192.168.1.0     | Lowest Host ID: 192.168.1.1   |                      |
| Broadcast Address:<br>192.168.1.63 | Highest Host ID: 192.168.1.62 |                      |

**Table 107** Subnet 2

| IP/SUBNET MASK                      | NETWORK NUMBER                 | LAST OCTET BIT VALUE |
|-------------------------------------|--------------------------------|----------------------|
| IP Address                          | 192.168.1.                     | 64                   |
| IP Address (Binary)                 | 11000000.10101000.00000001.    | 01000000             |
| Subnet Mask (Binary)                | 11111111.11111111.11111111.    | 11000000             |
| Subnet Address:<br>192.168.1.64     | Lowest Host ID: 192.168.1.65   |                      |
| Broadcast Address:<br>192.168.1.127 | Highest Host ID: 192.168.1.126 |                      |

**Table 108** Subnet 3

| IP/SUBNET MASK                      | NETWORK NUMBER                 | LAST OCTET BIT VALUE |
|-------------------------------------|--------------------------------|----------------------|
| IP Address                          | 192.168.1.                     | 128                  |
| IP Address (Binary)                 | 11000000.10101000.00000001.    | 10000000             |
| Subnet Mask (Binary)                | 11111111.11111111.11111111.    | 11000000             |
| Subnet Address:<br>192.168.1.128    | Lowest Host ID: 192.168.1.129  |                      |
| Broadcast Address:<br>192.168.1.191 | Highest Host ID: 192.168.1.190 |                      |

**Table 109** Subnet 4

| IP/SUBNET MASK                      | NETWORK NUMBER                 | LAST OCTET BIT VALUE |
|-------------------------------------|--------------------------------|----------------------|
| IP Address                          | 192.168.1.                     | 192                  |
| IP Address (Binary)                 | 11000000.10101000.00000001.    | 11000000             |
| Subnet Mask (Binary)                | 11111111.11111111.11111111.    | 11000000             |
| Subnet Address:<br>192.168.1.192    | Lowest Host ID: 192.168.1.193  |                      |
| Broadcast Address:<br>192.168.1.255 | Highest Host ID: 192.168.1.254 |                      |

## Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

**Table 110** Eight Subnets

| SUBNET | SUBNET ADDRESS | FIRST ADDRESS | LAST ADDRESS | BROADCAST ADDRESS |
|--------|----------------|---------------|--------------|-------------------|
| 1      | 0              | 1             | 30           | 31                |
| 2      | 32             | 33            | 62           | 63                |
| 3      | 64             | 65            | 94           | 95                |
| 4      | 96             | 97            | 126          | 127               |

**Table 110** Eight Subnets (continued)

| SUBNET | SUBNET ADDRESS | FIRST ADDRESS | LAST ADDRESS | BROADCAST ADDRESS |
|--------|----------------|---------------|--------------|-------------------|
| 5      | 128            | 129           | 158          | 159               |
| 6      | 160            | 161           | 190          | 191               |
| 7      | 192            | 193           | 222          | 223               |
| 8      | 224            | 225           | 254          | 255               |

## Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

**Table 111** 24-bit Network Number Subnet Planning

| NO. "BORROWED" HOST BITS | SUBNET MASK           | NO. SUBNETS | NO. HOSTS PER SUBNET |
|--------------------------|-----------------------|-------------|----------------------|
| 1                        | 255.255.255.128 (/25) | 2           | 126                  |
| 2                        | 255.255.255.192 (/26) | 4           | 62                   |
| 3                        | 255.255.255.224 (/27) | 8           | 30                   |
| 4                        | 255.255.255.240 (/28) | 16          | 14                   |
| 5                        | 255.255.255.248 (/29) | 32          | 6                    |
| 6                        | 255.255.255.252 (/30) | 64          | 2                    |
| 7                        | 255.255.255.254 (/31) | 128         | 1                    |

The following table is a summary for subnet planning on a network with a 16-bit network number.

**Table 112** 16-bit Network Number Subnet Planning

| NO. "BORROWED" HOST BITS | SUBNET MASK           | NO. SUBNETS | NO. HOSTS PER SUBNET |
|--------------------------|-----------------------|-------------|----------------------|
| 1                        | 255.255.128.0 (/17)   | 2           | 32766                |
| 2                        | 255.255.192.0 (/18)   | 4           | 16382                |
| 3                        | 255.255.224.0 (/19)   | 8           | 8190                 |
| 4                        | 255.255.240.0 (/20)   | 16          | 4094                 |
| 5                        | 255.255.248.0 (/21)   | 32          | 2046                 |
| 6                        | 255.255.252.0 (/22)   | 64          | 1022                 |
| 7                        | 255.255.254.0 (/23)   | 128         | 510                  |
| 8                        | 255.255.255.0 (/24)   | 256         | 254                  |
| 9                        | 255.255.255.128 (/25) | 512         | 126                  |
| 10                       | 255.255.255.192 (/26) | 1024        | 62                   |
| 11                       | 255.255.255.224 (/27) | 2048        | 30                   |
| 12                       | 255.255.255.240 (/28) | 4096        | 14                   |
| 13                       | 255.255.255.248 (/29) | 8192        | 6                    |

**Table 112** 16-bit Network Number Subnet Planning (continued)

| NO. "BORROWED"<br>HOST BITS | SUBNET MASK           | NO. SUBNETS | NO. HOSTS PER<br>SUBNET |
|-----------------------------|-----------------------|-------------|-------------------------|
| 14                          | 255.255.255.252 (/30) | 16384       | 2                       |
| 15                          | 255.255.255.254 (/31) | 32768       | 1                       |

## Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the ZyXEL Device.

Once you have decided on the network number, pick an IP address for your ZyXEL Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

### Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space*.

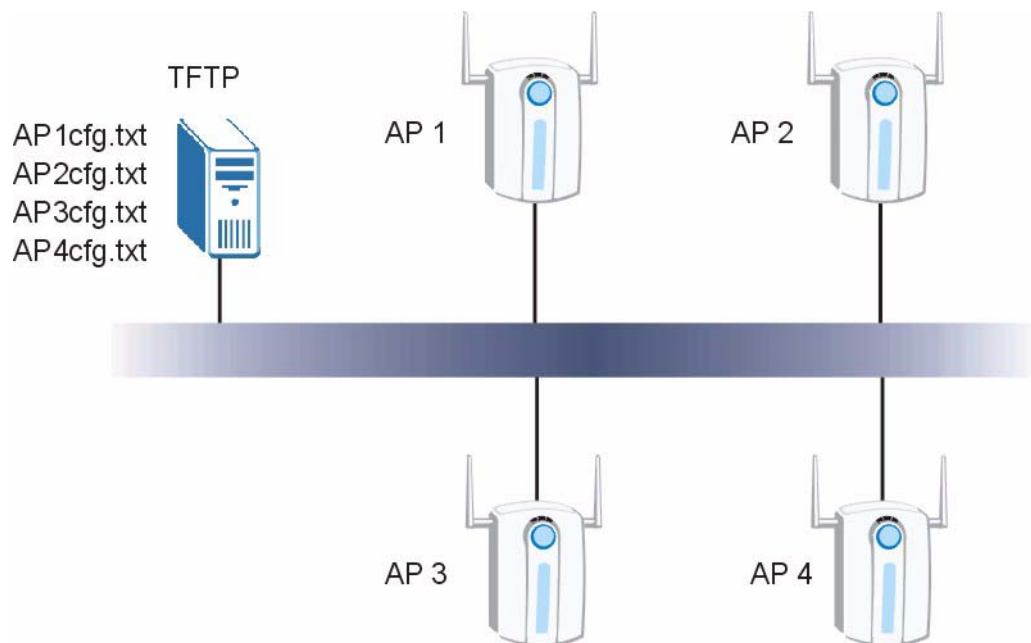
# Text File Based Auto Configuration

This chapter describes how administrators can use text configuration files to configure the wireless LAN settings for multiple APs.

## Text File Based Auto Configuration Overview

You can use plain text configuration files to configure the wireless LAN settings on multiple APs. The AP can automatically get a configuration file from a TFTP server at startup or after renewing DHCP client information.

**Figure 201** Text File Based Auto Configuration



Use one of the following methods to give the AP the IP address of the TFTP server where you store the configuration files and the name of the configuration file that it should download.

You can have a different configuration file for each AP. You can also have multiple APs use the same configuration file.



---

If adjacent APs use the same configuration file, you should leave out the channel setting since they could interfere with each other's wireless traffic.

---

## Auto Configuration by DHCP

A DHCP response can use options 66 and 67 to assign a TFTP server IP address and a filename. If the AP is configured as a DHCP client, these settings can be used to perform auto configuration.

**Table 113** Auto Configuration by DHCP

| COMMAND                              | DESCRIPTION   |
|--------------------------------------|---|
| wcfg autocfg dhcp [enable   disable] | Turn configuration of TFTP server IP address and filename through DHCP on or off. |

If this feature is enabled and the DHCP response provides a TFTP server IP address and a filename, the AP will try to download the file from the specified TFTP server. The AP then uses the file to configure wireless LAN settings.



---

Not all DHCP servers allow you to specify options 66 and 67.

---

## Manual Configuration

Use the following command to manually configure a TFTP server IP address and a file name for the AP to use for auto provisioning whenever the AP starts up. See [Section 24.1 on page 249](#) for how to access the Command Interpreter (CI).

**Table 114** Manual Configuration

| COMMAND                             | DESCRIPTION   |
|-------------------------------------|---|
| wcfg autocfg server [IP] [filename] | Specify the TFTP server IP address and file name from which the AP is to download a configuration file whenever the AP starts up. |

## Configuration Via SNMP

You can configure and trigger the auto configuration remotely via SNMP.

Use the following procedure to have the AP download the configuration file.

**Table 115** Configuration via SNMP

| STEPS  | MIB VARIABLE    | VALUE  |
|--------|-----------------|--|
| Step 1 | pwTftpServer    | Set the IP address of the TFTP server.         |
| Step 2 | pwTftpFileName  | Set the file name, for example, g3000hcfg.txt. |
| Step 3 | pwTftpFileType  | Set to 3 (text configuration file).            |
| Step 4 | pwTftpOpCommand | Set to 2 (download).                           |

## Verifying Your Configuration File Upload Via SNMP

You can use SNMP management software to display the configuration file version currently on the device by using the following MIB.

**Table 116** Displaying the File Version

| ITEM         | OBJECT ID               | DESCRIPTION   |
|--------------|-------------------------|---|
| pwCfgVersion | 1.3.6.1.4.1.890.1.9.1.2 | This displays the current configuration file version. |

## Troubleshooting Via SNMP

If you have any difficulties with the configuration file upload, you can try using the following MIB 10 to 20 seconds after using SNMP to have the AP download the configuration file.

**Table 117** Displaying the File Version

| ITEM           | OBJECT ID               | DESCRIPTION  |
|----------------|-------------------------|--|
| pwTftpOpStatus | 1.3.6.1.4.1.890.1.9.1.6 | This displays the current operating status of the TFTP client. |

## Configuration File Format

The text based configuration file must use the following format.

**Figure 202** Configuration File Format

```
!#ZYXEL PROWLAN
!#VERSION 12
wcfg security 1 xxx
wcfg security save
wcfg ssid 1 xxx
wcfg ssid save
```

The first line must be !#ZYXEL PROWLAN.

The second line must specify the file version. The AP compares the file version with the version of the last configuration file that it downloaded. If the version of the downloaded file is the same or smaller (older), the AP ignores the file. If the version of the downloaded file is larger (newer), the AP uses the file.

## Configuration File Rules

You can only use the `wlan` and `wcfg` commands in the configuration file. The AP ignores other ZyNOS commands but continues to check the next command.

The AP ignores any improperly formatted commands and continues to check the next line.

If there are any errors while processing the configuration file, the AP generates a message with the line number and reason for the first error (subsequent errors during the processing of an individual configuration file are not recorded). You can use SNMP management software to display the message by using the following MIB.

**Table 118** Displaying the Auto Configuration Status

| ITEM             | OBJECT ID               | DESCRIPTION                              |
|------------------|-------------------------|--|
| pwAutoCfgMessage | 1.3.6.1.4.1.890.1.9.1.9 | Auto configuration status message string |

The commands will be executed line by line just like if you entered them in a console or Telnet CI session. Be careful to ensure the integrity of the whole AP configuration. If there are existing settings in the AP, the newly loaded configuration file will either coexist with the previous settings or replace them.

You can zip each configuration file. You must use the store compression method and a .zip file extension. When zipping a configuration file, you can also add password protection using the same password that you use to log into the AP.

## Wcfg Command Configuration File Examples

These example configuration files use the `wcfg` command to configure security and SSID profiles.

**Figure 203** WEP Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 11
wcfg security 1 name Test-wep
wcfg security 1 security wep
wcfg security 1 wep keysize 64 ascii
wcfg security 1 wep key1 abcde
wcfg security 1 wep key2 bcdef
wcfg security 1 wep key3 cdefg
wcfg security 1 wep key4 defgh
wcfg security 1 wep keyindex 1
wcfg security save
wcfg ssid 1 name ssid-wep
wcfg ssid 1 security Test-wep
wcfg ssid 1 l2iolation disable
wcfg ssid 1 macfilter disable
wcfg ssid save
```

**Figure 204** 802.1X Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 12
wcfg security 2 name Test-8021x
wcfg security 2 mode 8021x-static128
wcfg security 2 wep key1 abcdefghijklm
wcfg security 2 wep key2 bcdefghijklmn
wcfg security 2 wep keyindex 1
wcfg security 2 reauthtime 1800
wcfg security 2 idletime 3600
wcfg security save
wcfg radius 2 name radius-rd
wcfg radius 2 primary 172.23.3.4 1812 1234 enable
wcfg radius 2 backup 172.23.3.5 1812 1234 enable
wcfg radius save
wcfg ssid 2 name ssid-8021x
wcfg ssid 2 security Test-8021x
wcfg ssid 2 radius radius-rd
wcfg ssid 2 qos 4
wcfg ssid 2 l2isolation disable
wcfg ssid 2 macfilter disable
wcfg ssid save
```

**Figure 205** WPA-PSK Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 13
wcfg security 3 name Test-wpapsk
wcfg security 3 mode wpapsk
wcfg security 3 passphrase qwertyuiop
wcfg security 3 reauthtime 1800
wcfg security 3 idletime 3600
wcfg security 3 groupkeytime 1800
wcfg security save
wcfg ssid 3 name ssid-wpapsk
wcfg ssid 3 security Test-wpapsk
wcfg ssid 3 qos 4
wcfg ssid 3 l2isolation disable
wcfg ssid 3 macfilter disable
wcfg ssid save
```

**Figure 206 WPA Configuration File Example**

```
!#ZYXEL PROWLAN
!#VERSION 14
wcfg security 4 name Test-wpa
wcfg security 4 mode wpa
wcfg security 4 reauthtime 1800
wcfg security 4 idletime 3600
wcfg security 4 groupkeytime 1800
wcfg security save
wcfg radius 4 name radius-rd1
wcfg radius 4 primary 172.0.20.38 1812 20 enable
wcfg radius 4 backup 172.0.20.39 1812 20 enable
wcfg radius save
wcfg ssid 4 name ssid-wpa
wcfg ssid 4 security Test-wpa
wcfg ssid 4 qos 4
wcfg ssid 4 l2isolation disable
wcfg ssid 4 macfilter disable
wcfg ssid save
```

### Wlan Command Configuration File Example

This example configuration file uses the `wlan` command to configure the AP to use the security and SSID profiles from the `wcfg` command configuration file examples and general wireless settings. You could actually combine all of this chapter's example configuration files into a single configuration file. Remember that the commands are applied in order. So for example, you would place the commands that create security and SSID profiles before the commands that tell the AP to use those profiles.

**Figure 207** Wlan Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 15
wcfg ssid 1 name ssid-wep
wcfg ssid 1 security Test-wep
wcfg ssid 2 name ssid-8021x
wcfg ssid 2 security Test-8021x
wcfg ssid 2 radius radius-rd
wcfg ssid 3 name ssid-wpapsk
wcfg ssid 3 security Test-wpapsk
wcfg ssid 4 name ssid-wpa2psk
wcfg ssid 4 security Test-wpa2psk
wcfg ssid save
!line starting with '!' is comment
!change to channel 8
wlan chid 8
!change operating mode -> AP mode,
!then select ssid-wep as running WLAN profile
wlan opmode 0
wlan ssidprofile ssid-wep
!change operating mode -> MBSSID mode,
!then select ssid-wpapsk, ssid-wpa2psk as running WLAN profiles
wlan opmode 3
wlan ssidprofile ssid-wpapsk ssid-wpa2psk
! set output power level to 50%
wlan output power 2
```



# Legal Information

## Copyright

Copyright © 2008 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

## Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

## Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

## Certifications

### Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- 1 Reorient or relocate the receiving antenna.
- 2 Increase the separation between the equipment and the receiver.
- 3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 4 Consult the dealer or an experienced radio/TV technician for help.



### FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

## 注意 !

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。  
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

在 5250MHz~5350MHz 頻帶內操作之無線資訊傳輸設備，限於室內使用。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。

### Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz and 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

**Viewing Certifications**

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

**ZyXEL Limited Warranty**

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

**Note**

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at [http://www.zyxel.com/web/support\\_warranty\\_info.php](http://www.zyxel.com/web/support_warranty_info.php).

**Registration**

Register your product online to receive e-mail notices of firmware upgrades and information at [www.zyxel.com](http://www.zyxel.com) for global products, or at [www.us.zyxel.com](http://www.us.zyxel.com) for North American products.



# Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional offices are listed below (see also [http://www.zyxel.com/web/contact\\_us.php](http://www.zyxel.com/web/contact_us.php)). Please have the following information ready when you contact an office.

## Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

“+” is the (prefix) number you dial to make an international telephone call.

## Corporate Headquarters (Worldwide)

- Support E-mail: [support@zyxel.com.tw](mailto:support@zyxel.com.tw)
- Sales E-mail: [sales@zyxel.com.tw](mailto:sales@zyxel.com.tw)
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: [www.zyxel.com](http://www.zyxel.com)
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

## China - ZyXEL Communications (Beijing) Corp.

- Support E-mail: [cso.zycn@zyxel.cn](mailto:cso.zycn@zyxel.cn)
- Sales E-mail: [sales@zyxel.cn](mailto:sales@zyxel.cn)
- Telephone: +86-010-82800646
- Fax: +86-010-82800587
- Address: 902, Unit B, Horizon Building, No.6, Zhichun Str, Haidian District, Beijing
- Web: <http://www.zyxel.cn>

## China - ZyXEL Communications (Shanghai) Corp.

- Support E-mail: [cso.zycn@zyxel.cn](mailto:cso.zycn@zyxel.cn)
- Sales E-mail: [sales@zyxel.cn](mailto:sales@zyxel.cn)
- Telephone: +86-021-61199055
- Fax: +86-021-52069033

- Address: 1005F, ShengGao International Tower, No.137 XianXia Rd., Shanghai
- Web: <http://www.zyxel.cn>

### **Costa Rica**

- Support E-mail: [soporte@zyxel.co.cr](mailto:soporte@zyxel.co.cr)
- Sales E-mail: [sales@zyxel.co.cr](mailto:sales@zyxel.co.cr)
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: [www.zyxel.co.cr](http://www.zyxel.co.cr)
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

### **Czech Republic**

- E-mail: [info@cz.zyxel.com](mailto:info@cz.zyxel.com)
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: [www.zyxel.cz](http://www.zyxel.cz)
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Česká Republika

### **Denmark**

- Support E-mail: [support@zyxel.dk](mailto:support@zyxel.dk)
- Sales E-mail: [sales@zyxel.dk](mailto:sales@zyxel.dk)
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: [www.zyxel.dk](http://www.zyxel.dk)
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

### **Finland**

- Support E-mail: [support@zyxel.fi](mailto:support@zyxel.fi)
- Sales E-mail: [sales@zyxel.fi](mailto:sales@zyxel.fi)
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: [www.zyxel.fi](http://www.zyxel.fi)
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

### **France**

- E-mail: [info@zyxel.fr](mailto:info@zyxel.fr)
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: [www.zyxel.fr](http://www.zyxel.fr)
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

**Germany**

- Support E-mail: [support@zyxel.de](mailto:support@zyxel.de)
- Sales E-mail: [sales@zyxel.de](mailto:sales@zyxel.de)
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: [www.zyxel.de](http://www.zyxel.de)
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

**Hungary**

- Support E-mail: [support@zyxel.hu](mailto:support@zyxel.hu)
- Sales E-mail: [info@zyxel.hu](mailto:info@zyxel.hu)
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: [www.zyxel.hu](http://www.zyxel.hu)
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

**India**

- Support E-mail: [support@zyxel.in](mailto:support@zyxel.in)
- Sales E-mail: [sales@zyxel.in](mailto:sales@zyxel.in)
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: <http://www.zyxel.in>
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

**Japan**

- Support E-mail: [support@zyxel.co.jp](mailto:support@zyxel.co.jp)
- Sales E-mail: [zyp@zyxel.co.jp](mailto:zyp@zyxel.co.jp)
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: [www.zyxel.co.jp](http://www.zyxel.co.jp)
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

**Kazakhstan**

- Support: <http://zyxel.kz/support>
- Sales E-mail: [sales@zyxel.kz](mailto:sales@zyxel.kz)
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: [www.zyxel.kz](http://www.zyxel.kz)
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

### **Malaysia**

- Support E-mail: [support@zyxel.com.my](mailto:support@zyxel.com.my)
- Sales E-mail: [sales@zyxel.com.my](mailto:sales@zyxel.com.my)
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: <http://www.zyxel.com.my>
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

### **North America**

- Support E-mail: [support@zyxel.com](mailto:support@zyxel.com)
- Support Telephone: +1-800-978-7222
- Sales E-mail: [sales@zyxel.com](mailto:sales@zyxel.com)
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: [www.zyxel.com](http://www.zyxel.com)
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

### **Norway**

- Support E-mail: [support@zyxel.no](mailto:support@zyxel.no)
- Sales E-mail: [sales@zyxel.no](mailto:sales@zyxel.no)
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: [www.zyxel.no](http://www.zyxel.no)
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

### **Poland**

- E-mail: [info@pl.zyxel.com](mailto:info@pl.zyxel.com)
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: [www.pl.zyxel.com](http://www.pl.zyxel.com)
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

### **Russia**

- Support: <http://zyxel.ru/support>
- Sales E-mail: [sales@zyxel.ru](mailto:sales@zyxel.ru)
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: [www.zyxel.ru](http://www.zyxel.ru)
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

**Singapore**

- Support E-mail: [support@zyxel.com.sg](mailto:support@zyxel.com.sg)
- Sales E-mail: [sales@zyxel.com.sg](mailto:sales@zyxel.com.sg)
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: <http://www.zyxel.com.sg>
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

**Spain**

- Support E-mail: [support@zyxel.es](mailto:support@zyxel.es)
- Sales E-mail: [sales@zyxel.es](mailto:sales@zyxel.es)
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: [www.zyxel.es](http://www.zyxel.es)
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

**Sweden**

- Support E-mail: [support@zyxel.se](mailto:support@zyxel.se)
- Sales E-mail: [sales@zyxel.se](mailto:sales@zyxel.se)
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: [www.zyxel.se](http://www.zyxel.se)
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

**Taiwan**

- Support E-mail: [support@zyxel.com.tw](mailto:support@zyxel.com.tw)
- Sales E-mail: [sales@zyxel.com.tw](mailto:sales@zyxel.com.tw)
- Telephone: +886-2-27399889
- Fax: +886-2-27353220
- Web: <http://www.zyxel.com.tw>
- Address: Room B, 21F., No.333, Sec. 2, Dunhua S. Rd., Da-an District, Taipei

**Thailand**

- Support E-mail: [support@zyxel.co.th](mailto:support@zyxel.co.th)
- Sales E-mail: [sales@zyxel.co.th](mailto:sales@zyxel.co.th)
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: <http://www.zyxel.co.th>
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

### **Turkey**

- Support E-mail: [cso@zyxel.com.tr](mailto:cso@zyxel.com.tr)
- Telephone: +90 212 222 55 22
- Fax: +90-212-220-2526
- Web: <http://www.zyxel.com.tr>
- Address: Kaptanpasa Mahallesi Piyalepasa Bulvari Ortadogu Plaza N:14/13 K:6 Okmeydani/Sisli Istanbul/Turkey

### **Ukraine**

- Support E-mail: [support@ua.zyxel.com](mailto:support@ua.zyxel.com)
- Sales E-mail: [sales@ua.zyxel.com](mailto:sales@ua.zyxel.com)
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: [www.ua.zyxel.com](http://www.ua.zyxel.com)
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

### **United Kingdom**

- Support E-mail: [support@zyxel.co.uk](mailto:support@zyxel.co.uk)
- Sales E-mail: [sales@zyxel.co.uk](mailto:sales@zyxel.co.uk)
- Telephone: +44-1344-303044, 0845 122 0301 (UK only)
- Fax: +44-1344-303034
- Web: [www.zyxel.co.uk](http://www.zyxel.co.uk)
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

# Index

## A

access [34](#)  
 access point [34](#)  
 access privileges [36](#)  
 address assignment [133](#)  
 address filtering [33](#)  
 administrator authentication on RADIUS [80](#)  
 Advanced Encryption Standard  
   See AES.  
 AES [290](#)  
 alternative subnet mask notation [303](#)  
 antenna [261](#)  
   directional [293](#)  
   gain [293](#)  
   omni-directional [293](#)  
 AP [33](#), [34](#), [35](#), [137](#), [283](#)  
 AP+Bridge [33](#), [35](#)  
 applications [33](#)  
   Access Point [34](#)  
   AP/Bridge [35](#)  
   Bridge/Repeater [34](#)  
   MBSSID [36](#)  
 ATC [87](#), [119](#)  
 ATC+WMM [119](#)  
 ATM [87](#)  
 authentication server [33](#)  
 auto configuration [309](#)  
 auto configuration status [312](#)

## B

backup [220](#)  
 Basic Service Set  
   see BSS  
 bridge [34](#), [35](#)  
 Bridge Protocol Data Units (BPDUs) [91](#)  
 Bridge/Repeater [33](#), [34](#)  
 BSS [36](#), [281](#)  
 BSSID [33](#)

## C

CA [288](#)  
 Certificate Authority  
   See CA.  
 certificates [162](#)  
   thumbprint algorithms [170](#)  
   thumbprints [170](#)  
   verifying fingerprints [170](#)  
 certifications [317](#)  
   notices [318](#)  
   viewing [319](#)  
 channel [33](#), [283](#)  
   interference [283](#)  
 CI commands [250](#)  
 Class of Service (CoS) [89](#)  
 collision [238](#)  
 command interface [38](#)  
 command interpreter [249](#)  
 configuration [33](#)  
 configuration file  
   examples [312](#)  
   format [311](#)  
 configuration file rules [312](#)  
 contact information [321](#)  
 copyright [317](#)  
 CoS [89](#)  
 CPU load [238](#)  
 CTS (Clear to Send) [284](#)  
 customer support [321](#)

## D

default [222](#)  
 DFS [91](#)  
 DHCP [240](#)  
 diagnostic [241](#)  
 diagnostic tools [237](#)  
 Differentiated Services [89](#)  
 DiffServ [89](#)  
 DiffServ Code Point (DSCP) [89](#)  
 DiffServ Code Points [89](#)  
 DiffServ marking rule [89](#)

disclaimer [317](#)  
DS field [89](#)  
DSCPs [89](#)  
Dynamic Frequency Selection [91](#)  
dynamic WEP key exchange [289](#)

## E

EAP authentication [287](#)  
encryption [35](#), [290](#)  
error log [240](#)  
error/information messages  
    sample [241](#)  
ESS [282](#)  
ESSID [260](#)  
Extended Service Set  
    see ESS  
Extended Service Set IDentification [94](#), [116](#)

## F

FCC interference statement [317](#)  
file version [311](#)  
filename conventions [243](#)  
filtering [33](#)  
firmware file  
    maintenance [217](#)  
flow control [225](#)  
fragmentation threshold [284](#)  
friendly AP list [140](#)  
FTP [38](#), [143](#), [147](#), [254](#)  
    restrictions [143](#), [254](#)

## G

general setup [79](#), [231](#)  
guest SSID [37](#)

## H

hidden menus [229](#)  
hidden node [283](#)  
honeypot attack [138](#)

host [81](#)  
HTTPS [148](#)  
    example [150](#)  
humidity [261](#)

## I

IANA [308](#)  
IBSS [281](#)  
IEEE 802.11g [285](#)  
IEEE 802.1x [33](#)  
in-band management [199](#)  
Independent Basic Service Set [217](#)  
    see IBSS  
initial screen [225](#)  
initialization vector (IV) [290](#)  
installation [33](#)  
interference [33](#)  
internal authentication server [33](#)  
Internet access [233](#)  
Internet Assigned Numbers Authority  
    See IANA  
Internet security gateway [33](#)  
Internet telephony [36](#)  
IP address [133](#), [134](#), [234](#), [240](#), [242](#), [262](#)  
IPSec VPN capability [263](#)  
isolation [33](#)

## L

layer-2 isolation [33](#), [37](#)  
link type [238](#)  
log and trace [241](#)  
log descriptions [190](#)  
login screen [226](#)  
logs [187](#)

## M

MAC address [33](#), [126](#)  
MAC address filter action [127](#), [128](#)  
MAC filter [37](#), [126](#)  
MAC filtering [263](#)  
MAC service data unit [93](#), [97](#), [116](#)  
main menu [229](#)

maintenance [33](#)  
 management [33](#)  
 Management Information Base (MIB) [155](#)  
 management VLAN [199](#)  
 managing the device  
   good habits [39](#)  
   using FTP. See FTP.  
   using Telnet. See command interface.  
   using the command interface. See command interface.  
 max age [91](#)  
 MBSSID [33](#), [36](#)  
 Message Integrity Check (MIC) [290](#)  
 mobile access [33](#)  
 mode [33](#)  
 MSDU [93](#), [97](#), [116](#)

## N

NAT [308](#)  
 network [33](#)  
 network access [33](#)  
 network bridge [34](#)  
 network traffic [33](#)

## O

operating mode [33](#)  
 out-of-band management [199](#)

## P

packets [238](#)  
 Pairwise Master Key (PMK) [290](#), [291](#)  
 password [80](#), [226](#), [227](#), [262](#)  
 path cost [90](#)  
 Per-Hop Behavior [89](#)  
 PHB (Per-Hop Behavior) [89](#)  
 ping [242](#)  
 PoE [265](#)  
 power specification [261](#)  
 power specifications [265](#)  
 preamble mode [285](#)  
 pre-configured profiles [37](#)  
 priorities [87](#)

prioritization [33](#)  
 private IP address [133](#)  
 product registration [319](#)  
 PSK [290](#)

## Q

QoS [33](#), [119](#)  
 Quick Start Guide [41](#)

## R

radio [33](#)  
 RADIUS [286](#)  
   message types [287](#)  
   messages [287](#)  
   shared secret key [287](#)  
 rapid STP [90](#)  
 RAS [239](#)  
 rate  
   receiving [238](#)  
   transmission [238](#)  
 reauthentication time [106](#), [107](#), [108](#), [109](#), [110](#)  
 registration  
   product [319](#)  
 related documentation [3](#)  
 remote management  
   how SSH works [144](#)  
   HTTPS [148](#)  
   HTTPS example [150](#)  
   SSH [144](#)  
   SSH implementation [145](#)  
   Telnet [145](#)  
 remote management limitations [143](#), [254](#)  
 remote management setup [253](#)  
 remote node [238](#)  
 repeater [34](#)  
 required fields [229](#)  
 restore [220](#)  
 restore configuration [246](#)  
 RF interference [33](#)  
 roaming [129](#)  
   requirements [130](#)  
 rogue AP [33](#), [137](#), [138](#), [139](#), [140](#), [141](#)  
 rogue AP list [141](#)  
 root bridge [90](#)  
 RTS (Request To Send) [284](#)  
   threshold [283](#), [284](#)

RTS/CTS handshake [93, 97, 116](#)

## S

safety warnings [6](#)

security [34](#)

security profiles [33](#)

server [33](#)

Service Set [94, 116](#)

Service Set Identifier  
see SSID

SMT [228](#)

SMT menu overview [228](#)

SNMP [154, 263](#)

manager [155](#)

MIBs [156](#)

traps [157](#)

version 3 and security [157](#)

Spanning Tree Protocol [90](#)

specifications [265](#)

SSH [144](#)

how SSH works [144](#)

implementation [145](#)

SSID [36](#)

SSID profile [118](#)

pre-configured [36](#)

SSID profiles [36, 37](#)

STP [90](#)

STP - how it works [91](#)

STP (Spanning Tree Protocol) [262](#)

STP path costs [90](#)

STP port states [91](#)

STP terminology [90](#)

subnet [301](#)

subnet mask [234, 240, 262, 302](#)

subnetting [304](#)

syntax conventions [4](#)

system

console port speed [240](#)

diagnostic [241](#)

log and trace [240](#)

system information [239](#)

system status [237](#)

time and date [251](#)

system information [238](#)

system information & diagnosis [237](#)

system maintenance [237, 239, 245, 247, 249, 251](#)

system name [79](#)

system timeout [144, 255](#)

## T

tagged VLAN example [199](#)

TCP/IP [242](#)

Telnet [145](#)

telnet [145, 252](#)

telnet configuration [252](#)

temperature [261](#)

Temporal Key Integrity Protocol (TKIP) [290](#)

terminal emulation [225](#)

text file based auto configuration [263, 309](#)

TFTP

restrictions [254](#)

TFTP file transfer [247](#)

TFTP restrictions [143](#)

time and date setting [251](#)

time setting [82](#)

time zone [252](#)

time-sensitive [33](#)

ToS [89](#)

trace records [240](#)

trademarks [317](#)

traffic security [33](#)

Type of Service [89](#)

## U

use [33](#)

## V

Virtual Local Area Network [195](#)

VLAN [195](#)

VoIP [33, 36, 119](#)

VoIP SSID [37](#)

VT100 [225](#)

## W

warranty [319](#)

note [319](#)

wcfg command [312](#)

WDS [34, 35, 94](#)

web [149](#)

- web configurator [33](#), [41](#), [43](#)
- WEP [33](#)
- WEP encryption [105](#)
- Wi-Fi Multimedia QoS [86](#)
- Wi-Fi Protected Access [33](#), [289](#)
- wired network [33](#), [34](#)
- wireless channel [260](#)
- wireless client WPA supplicants [291](#)
- Wireless Distribution System (WDS) [35](#)
- wireless Internet connection [34](#)
- wireless LAN [260](#)
- wireless security [36](#), [260](#), [285](#)
- WLAN
  - interference [283](#)
  - security parameters [292](#)
- WLAN interface [33](#)
- WMM [119](#)
- WPA [33](#), [289](#)
  - key caching [290](#)
  - pre-authentication [290](#)
  - user authentication [290](#)
  - vs WPA-PSK [290](#)
  - wireless client supplicant [291](#)
  - with RADIUS application example [291](#)
- WPA2 [33](#), [289](#)
  - user authentication [290](#)
  - vs WPA2-PSK [290](#)
  - wireless client supplicant [291](#)
  - with RADIUS application example [291](#)
- WPA2-Pre-Shared Key [289](#)
- WPA2-PSK [289](#), [290](#)
  - application example [291](#)
- WPA-PSK [289](#), [290](#)
  - application example [291](#)

## Z

- ZyNOS [244](#)
- ZyNOS F/W version [244](#)

